

**On the field isomorphism problem  
of generic polynomials  
via formal Tschirnhausen transformation**

**Hoshi, Akinari**

**星 明考**

**(Rikkyo University)**

**立教大学**

**Miyake, Katsuya**

**三宅 克哉**

**(Waseda University)**

**早稻田大学**

**2008/9/9**

## §1 Introduction

- What is **generic polynomial** ?
- **Field isomorphism problem**

## §2 Results: the cubic case

## §3 Proof of the results

(via formal Tschirnhausen transformation)

## §4 Application of the results:

a parametrized family of cubic Thue equations

---

## §5 Some numerical examples: the quintic case

## §1 Introduction

$G$  ; finite group,       $k$  ; arbitrary field

**Definition (generic polynomial)**

$f(t_1, \dots, t_n; X) \in k(t_1, \dots, t_n)[X]$

is a  $k$ -generic polynomial for  $G$

$\overset{\text{def}}{\iff}$

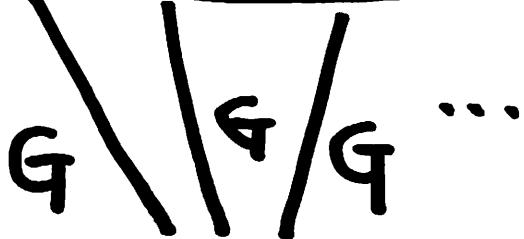
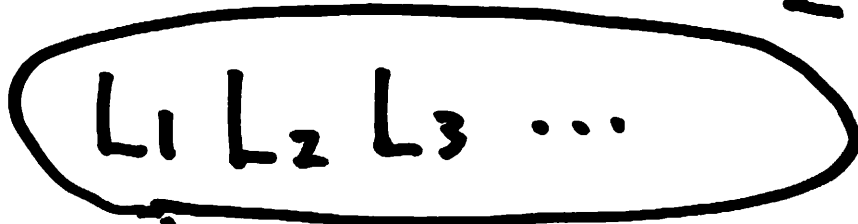
$$\left\{ \begin{array}{l} \text{(G1)} \quad \text{Gal}(f/k(t_1, \dots, t_n)) \cong G; \\ \text{(G2)} \quad \forall G\text{-Galois extension } L/K \supset k, \\ \quad \exists \vec{a} \in K^n \text{ s.t. } L = \text{Spl}_K f(\vec{a}; X) \end{array} \right.$$

$\exists$  specialization

$$\vec{t} \mapsto \vec{a} \in K^n$$

$\mathbb{R}$ -generic poly.

all  $G$ -Galois ext.



$$f(t_1, \dots, t_n; X)$$

$$\mathbb{R}(t_1, \dots, t_n)$$

## **Examples of $k$ -generic polynomials**

$k \ni \zeta_n$  ; primitive  $n$ -th root of unity

$X^n - t$  is  $k$ -generic for  $C_n$  (Kummer theory)

$\text{char } k = p > 0$

$X^p - X - t$  is  $k$ -generic for  $C_n$  (Artin-Schreier theory)

$k$  ; any  $k$ -generic for  $S_n$  with  $n - 2$  parameters

$$X^n + 0 \cdot X^{n-1} + s_2 X^{n-2} + \cdots + s_{n-2} X^2 + s_{n-1} X + s_{n-1}$$

$G \subset S_n$  ; transitive

**Examples** of  $k$ -generic polynomials  $f^G(X)$  for  $G$

$$f_s^{S_3}(X) = X^3 + sX + s, \quad (k; \text{any})$$

$$f_t^{C_3}(X) = X^3 - tX^2 - (t + 3)X - 1, \quad (k; \text{any})$$


---

$$f_{s,t}^{S_4}(X) = X^4 + sX^2 + tX + t, \quad (k; \text{any})$$

$$f_{s,t}^{D_4}(X) = X^4 + sX^2 + t, \quad (k; \text{char } k \neq 2)$$

$$f_{s,u}^{C_4}(X) = X^4 + sX^2 + \frac{s^2}{u^2 + 4}, \quad (k; \text{char } k \neq 2)$$

$D_n$  ; dihedral group of degree  $n$ , ( $\#D_n = 2n$ )

$C_n$  ; cyclic group of degree  $n$ ,

$G \subset S_5$  ; transitive,  **$S_5$ -generic** polynomial

$$f_{s,t}^{S_5}(X) = X^5 + sX^3 + tX + t, \quad (k; \text{any})$$

$F_{20}$  ; Frobenius group of order 20 ( $F_{20} \cong C_5 \rtimes C_4$ )

————— **Lecacheux's  $F_{20}$ -generic** polynomial (char  $k \neq 2$ ) —————

$$f_{p,q}^{F_{20}}(X) = X^5 + \left( r^2(p^2 + 4) - 2p - \frac{17}{4} \right) X^4 + \left( (p^2 + 4)(3r + 1) + \frac{13p}{2} + 1 \right) X^3 \\ - \left( r(p^2 + 4) + \frac{11p}{2} - 8 \right) X^2 + (p - 6)X + 1$$

————— **Brumer's  $D_5$ -generic** polynomial ( $k$  ; any) —————

$$f_{s,t}^{D_5}(X) = X^5 + (t - 3)X^4 + (s - t + 3)X^3 + (t^2 - t - 2s - 1)X^2 + sX + t$$

————— **Hashimoto-Tsunogai's  $C_5$ -generic** polynomial (char  $k \neq 2$ ) —————

$$f_{A,B}^{C_5}(X) = X^5 - \frac{P}{Q^2} (A^2 - 2A + 15B^2 + 2)X^3 + \frac{P^2}{Q^3} (2BX^2 - (A - 1)X - 2B),$$

where

$$P = (A^2 - A - 1)^2 + 25(A^2 + 1)B^2 + 125B^4, \quad Q = (A + 7)B^2 - A + 1$$

[Generic polynomials (book, 2002)] by Jensen-Ledet-Yui

$f_t^G(X) \in k(\overrightarrow{t})[X]$ ;  **$k$ -generic** for  $G$

$\stackrel{\text{def}}{\iff}$  (G1)  $\text{Gal}(f_t^G(X)/k(\overrightarrow{t})) \cong G$ ;

(G2)  $\forall G$ -Galois  $L/K \supset k$ ,

$\exists \overrightarrow{a} \in K^n$  s.t.  $L = \text{Spl}_K f(\overrightarrow{a}; X)$

**Kemper's Theorem (2001)** Over infinite field  $K$ ,

(G2)  $\iff$  (G3)  $\forall H \leq G$ ,  $\forall H$ -Galois  $L/K \supset k$ ,

$\exists \overrightarrow{a} \in K^n$  s.t.  $L = \text{Spl}_K f(\overrightarrow{a}; X)$

**DeMeyer (1983)** gave the definition by (G1)&(G3) and

proved that if  $K$  is infinite,  $\exists f_s^G(X)$  satisfying (G1)&(G3)

$\iff \exists$  (Saltman's) generic extension  $/K$  for  $G$

•  $K = k = \mathbb{F}_2, G = C_3$

$$f_t^{C_3}(X) := X^3 - tX^2 - (t + 3)X - 1 \in k(t)[X]$$

is  $\mathbb{F}_2$ -generic for  $C_3$  (i.e. satisfies (G1)&(G2))

**BUT** it does not satisfy (G3) because

$$f_0^{C_3}(X); \text{ irreducible } / \mathbb{F}_2$$

$$f_1^{C_3}(X); \text{ irreducible } / \mathbb{F}_2$$

**DeMeyer-McKenzie (2003) showed**

$\nexists f_s^G(X)$  satisfying (G1)&(G3) for  $K = \mathbb{F}_2$  and  $G = C_3$

## Some problems

$f_t^G(X)$  ;  $k$ -generic polynomial for  $G$

with  $n$  parameters  $t = (t_1, \dots, t_n)$

$L_a := \text{Spl}_K f_a^G(X)$  for  $a = (a_1, \dots, a_n) \in K^n$

Assume  $f_a^G(X)$  is separable (i.e. has no multiple root)

Because  $f_t^G(X)$  covers **all**  $G$ -Galois extensions over  $K \supset k$  by specializing parameters, it is natural to ask **the overlap**:

## Field isomorphism problem of $f_t^G(X)$

Determine whether  $L_a \cong L_b$  or not for  $a, b \in K^n$

$f_t^G(X)$  ;  $k$ -generic for  $G$

$L_a := \text{Spl}_K f_a^G(X)$  for  $a = (a_1, \dots, a_n) \in K^n$

By Kemper's Theorem, if  $\#K = \infty$ , for  $H \leq G$ ,  
 $f_t^G(X)$  also covers **all**  $H$ -Galois extensions over  $K$

Hence the following two problems naturally arise:

**Subfield problem** of  $f_t^G(X)$

Determine whether  $L_a \subset L_b$  for  $a, b \in K^n$

**Field intersection problem** of  $f_t^G(X)$

Determine  $L_a \cap L_b$  for  $a, b \in K^n$

$$L_a := \text{Spl}_K f_a^G(X) \text{ for } a = (a_1, \dots, a_n) \in K^n$$

Moreover we want to know

$K$  ; number field

**Isom( $\infty$ )** : For a fixed  $a = (a_1, \dots, a_n) \in K^n$ ,  
 $\exists? \infty b = (b_1, \dots, b_n) \in K^n$  s.t.  $L_a = L_b$  ?

$\mathcal{O}_K$  ; ring of integers in  $K$

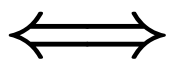
**Isom(Int, $\infty$ )** : For a fixed  $a = (a_1, \dots, a_n) \in (\mathcal{O}_K)^n$ ,  
 $\exists? \infty b = (b_1, \dots, b_n) \in (\mathcal{O}_K)^n$  s.t.  $L_a = L_b$  ?

## §2 Results: the cubic case

**Thm. 1 (H. - Miyake)** Assume that  $\text{char } k \neq 3$ .

Let  $f_s^{S_3}(X) := X^3 + sX + s \in k(s)[X]$ .

For  $a, b \in K$ ,  $\text{Spl}_K f_a^{S_3}(X) = \text{Spl}_K f_b^{S_3}(X)$



**Thm. 1 (H. - Miyake)** Assume that  $\text{char } k \neq 3$ .

Let  $f_s^{S_3}(X) := X^3 + sX + s \in k(s)[X]$ .

For  $a, b \in K$ ,  $\text{Spl}_K f_a^{S_3}(X) = \text{Spl}_K f_b^{S_3}(X)$

$\iff \exists u \in K$  s.t.

$$b = \frac{a(u^2 + 9u - 3a)^3}{(u^3 - 2au^2 - 9au - 2a^2 - 27a)^2}$$

**Thm. 1 (H. - Miyake)** Assume that  $\text{char } k \neq 3$ .

Let  $f_s^{S_3}(X) := X^3 + sX + s \in k(s)[X]$ .

For  $a, b \in K$ ,  $L_a = L_b$   $(L_a := \text{Spl}_K f_a^{S_3}(X))$

$\iff \exists u \in K$  s.t.

$$b = \frac{a(u^2 + 9u - 3a)^3}{(u^3 - 2au^2 - 9au - 2a^2 - 27a)^2}$$

Let  $K$  be a number field.

Applying Hilbert Irreducibility Theorem to **Thm. 1** /  $K(u)$ ,  
 $\exists \infty u \in K$  s.t.  $f_b(X)$  is well-defined & irreducible /  $K$

**Cor. Isom( $\infty$ )**

For a given  $a \in K$ ,  $\exists \infty b \in K$  s.t.  $L_a = L_b$

**Thm. 1 (H. - Miyake)** Assume that  $\text{char } k \neq 3$ .

Let  $f_s^{S_3}(X) := X^3 + sX + s \in k(s)[X]$ .

For  $a, b \in K$ ,  $L_a = L_b$   $(L_a := \text{Spl}_K f_a^{S_3}(X))$

$\iff \exists u \in K$  s.t.

$$b = \frac{a(u^2 + 9u - 3a)^3}{(u^3 - 2au^2 - 9au - 2a^2 - 27a)^2}$$

Let  $K$  be a number field and  $\mathcal{O}_K$  the ring of integers in  $K$ .

**Theorem (Siegel, 1929)**

If a rational function  $\varphi(u) \in K(u)$  has at least three distinct poles, then there are only finitely many  $u \in K$

s.t.  $\varphi(u) \in \mathcal{O}_K$

**Thm. 1 (H. - Miyake)** Assume that  $\text{char } k \neq 3$ .

Let  $f_s^{S_3}(X) := X^3 + sX + s \in k(s)[X]$ .

For  $a, b \in K$ ,  $L_a = L_b$  ( $L_a := \text{Spl}_K f_a^{S_3}(X)$ )

$\iff \exists u \in K$  s.t.

$$b = \frac{a(u^2 + 9u - 3a)^3}{(u^3 - 2au^2 - 9au - 2a^2 - 27a)^2}$$

Applying Siegel's Theorem to **Thm. 1**

$K$  ; a number field,  $\mathcal{O}_K$ ; the ring of integers in  $K$

**Cor. Isom(Int,  $\infty$ )** For a given  $a \in \mathcal{O}_K$ ,

$\exists$  only finitely many  $b \in \mathcal{O}_K$  s.t.  $L_a = L_b$

- For a given  $a \in \mathcal{O}_K$ ,  
all  $b \in \mathcal{O}_K$  with  $L_a = L_b$  can be obtained effectively.

**Example**  $K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}$

For  $-10 \leq a \leq 10$  and  $b \in \mathbb{Z}$ ,

$$L_a = L_b \quad (a \neq b) \iff$$

$$L_{-10} = L_{-106480} = L_{-400}, \quad L_{-9} = L_{-3087} = L_{-27},$$

$$L_{-7} = L_{-1588867} = L_{-189} = L_{-49},$$

$$L_{-6} = L_{12} = L_{54} = L_{48000}, \quad L_{-5} = L_{625},$$

$$L_{-4} = L_{128}, \quad L_{-3} = L_{27}, \quad L_{-2} = L_{3456},$$

$$L_1 = L_{300763}, \quad L_2 = L_{208974222}, \quad L_4 = L_{3456000}$$

For  $C_3$ , we take  $k$ -generic polynomial

$$f_t^{C_3}(X) := X^3 - tX^2 - (t + 3)X - 1 \in k(t)[X]$$

which is called Shanks' simplest cubic polynomial

**Thm. 2 (H. - Miyake)** Assume that  $\text{char } k \neq 2$ .

Let  $f_t^{C_3}(X) := X^3 - tX^2 - (t + 3)X - 1 \in k(t)[X]$ .

For  $m, n \in K$ ,  $\text{Spl}_K f_m^{C_3}(X) = \text{Spl}_K f_n^{C_3}(X)$

$$\iff \exists z \in K \text{ s.t. either } n = \frac{m(z^3 - 3z - 1) - 9z(z + 1)}{mz(z + 1) + z^3 + 3z^2 - 1}$$

$$\text{or } n = -\frac{m(z^3 + 3z^2 - 1) + 3(z^3 - 3z - 1)}{mz(z + 1) + z^3 + 3z^2 - 1}$$

**Remark** In the case of  $C_3$ , Morton (1994) and Chapman (1996) gave a similar result as a generalization of Kummer theory (without cubic root of unity)

**Thm. 2 (H. - Miyake)** Assume that  $\text{char } k \neq 2$ .

Let  $f_t^{C_3}(X) := X^3 - tX^2 - (t + 3)X - 1 \in k(t)[X]$ .

For  $m, n \in K$ ,

$$\text{Spl}_K f_m^{C_3}(X) = \text{Spl}_K f_n^{C_3}(X)$$

$$\iff \exists z \in K \text{ s.t. either } n = \frac{m(z^3 - 3z - 1) - 9z(z + 1)}{mz(z + 1) + z^3 + 3z^2 - 1}$$

$$\text{or } n = -\frac{m(z^3 + 3z^2 - 1) + 3(z^3 - 3z - 1)}{mz(z + 1) + z^3 + 3z^2 - 1}$$

**Cor. Isom( $\infty$ )** Let  $K \supset k$  be a number field.

For  $m \in K$ ,  $\exists \infty n \in K$  s.t.  $\text{Spl}_K f_m^{C_3}(X) = \text{Spl}_K f_n^{C_3}(X)$

**Cor. Isom(Int, $\infty$ )** Let  $K \supset k$  be a number field.

For  $m \in \mathcal{O}_K$ ,  $\exists$  only finitely many  $n \in \mathcal{O}_K$  s.t.

$$\text{Spl}_K f_m^{C_3}(X) = \text{Spl}_K f_n^{C_3}(X)$$

**Example**  $K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}, L_m = \text{Spl}_{\mathbb{Q}} f_m^{C_3}(X)$

• Note that  $L_{-m-3} = L_m$

For  $-1 \leq a \leq 10$  and  $-1 \leq b \in \mathbb{Z}$ ,

$L_a = L_b$  ( $a \neq b$ )  $\iff$

$$L_{-1} = L_5 = L_{12} = L_{1259},$$

$$L_0 = L_3 = L_{54},$$

$$L_1 = L_{66},$$

$$L_2 = L_{2389}$$

### §3 Proof of the results

(via formal Tschirnhausen transformation)

Note first that, for **fixed**  $a, b \in K^n$ , an **algorithm** to the

$\left\{ \begin{array}{l} \text{field isomorphism problem } (L_a \cong L_b ?) \\ \text{subfield problem } (L_a \subset L_b ?) \\ \text{field intersection problem } (L_a \cap L_b = ?) \end{array} \right.$

of  $f_t^G(X)$  always **exists** !

→ Using resolvent polynomials (well-known)

**BUT** an algorithm **does not know**

the structure of all  $G$ -Galois extensions

**For example (well-known method)**

$$f_{s,t}^{D_5}(X) = X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2-t-2s-1)X^2 + sX + t$$

**For  $\mathbf{a} = (a_1, a_2), \mathbf{b} = (b_1, b_2) \in K^2,$**

**assume  $f_{\mathbf{a}}^{D_5}(X), f_{\mathbf{b}}^{D_5}(X)$  ; irreducible (Gal  $\cong D_5$  or  $C_5$ )**

---

**For example, we take  $K = \mathbb{Q}$**

**$\mathbf{a} = (0, 1), \mathbf{b} = (1, 1), \mathbf{c} = (-1, 1)$  then Gal  $\cong D_5$  and**

- **$\text{Spl}_{\mathbb{Q}} f_{\mathbf{a}}^{D_5}(X) \neq \text{Spl}_{\mathbb{Q}} f_{\mathbf{b}}^{D_5}(X)$**
- **$\text{Spl}_{\mathbb{Q}} f_{\mathbf{a}}^{D_5}(X) = \text{Spl}_{\mathbb{Q}} f_{\mathbf{c}}^{D_5}(X)$**

Put  $F_{a,b}^{D_5}(Z) := \text{Resultant}_Y(f_a^{D_5}(Y), f_b^{D_5}(Z - hY))$

“ $Z = X + hY$ ” ; degree 25 ( $\uparrow$  resolvent polynomial)

We can choose  $h \in \mathbb{Z}$  as  $F_{a,b}^{D_5}(X)$  has **no** repeated factor

Then

decomposition type (DT) of  $F_{a,b}^{D_5}(X)$  over  $K$  is given by

$$\mathbf{DT}(F_{a,b}^{D_5}) = \begin{cases} (5)(5)(5)(5)(5), & \text{if } L_a = L_b, \text{Gal}_K f_a^{D_5}(X) \cong C_5 \\ (5)(10)(10), & \text{if } L_a = L_b, \text{Gal}_K f_a^{D_5}(X) \cong D_5 \\ (25), & \text{otherwise} \end{cases}$$

$$L_a := \text{Spl}_K f_a^{D_5}(X) \text{ for } \mathbf{a} = (a_1, a_2) \in K^2$$

**Resolvent polynomial (well-known method)** (cf. Cohen's book GTM138)

$\overline{K}$  ; (fixed) alg. closure of  $K$ ,

$f(X) = \prod_{i=1}^m (X - \alpha_i)$ ; degree  $m$  with fixed ordering of  $\alpha_i \in \overline{K}$ ,

$H \leq G \leq S_m$ ,

For  $\Theta \in k[x_1, \dots, x_m]$  ;  $G$ -primitive  $H$ -invariant, i.e.  $H = \text{Stab}_G(\Theta)$ ,

surjective specialization homomorphism

$$\begin{aligned} \omega_f : k[x_1, \dots, x_m] &\rightarrow k(\alpha_1, \dots, \alpha_m); \\ \Theta(x_1, \dots, x_m) &\mapsto \Theta(\alpha_1, \dots, \alpha_m) \end{aligned}$$

$$\mathcal{RP}_{\Theta, G}(X) := \prod_{\overline{\pi} \in G/H} (X - \pi(\Theta)) \in k(x_1, \dots, x_m)^G[X];$$

is called **formal**  $G$ -relative  $H$ -invariant **resolvent** by  $\Theta$

$$\mathcal{RP}_{\Theta, G, f}(X) := \prod_{\overline{\pi} \in G/H} (X - \omega_f(\pi(\Theta)));$$

is called  $G$ -relative  $H$ -invariant **resolvent** of  $f$  by  $\Theta$

**Assume that  $\text{Gal}_K f(X) \leq G$**

**$\mathcal{RP}_{\Theta, G, f}(X) = \prod_{i=1}^l h_i^{e_i}(X)$  ; irreducible decomp. /  $K$**

**Then there exists a bijection**

$$\text{Gal}(f) \backslash G / H \quad \longleftrightarrow \quad \{h_1^{e_1}(X), \dots, h_l^{e_l}(X)\}$$

$$\text{Gal}(f) \pi H \quad \longmapsto \quad h_\pi(X) = \prod_{\tau H \subseteq \text{Gal}(f) \pi H} (X - \omega_f(\tau(\Theta)))$$

**For a  $k$ -generic polynomial  $f_t^G(X)$  for  $G$ ,**

**we can apply  $f = f_a^G(X) f_b^G(X)$ ,**

**some suitable  $G \leq S_n \times S_n \leq S_m$  and  $H \leq G$**

**( $\rightarrow$  called multi-resolvent)**

• The case of  $G = S_n \times S_n$

$$f = f_a^{S_n}(X) f_b^{S_n}(X), (a, b \in K^r)$$

$\Delta(S_n \times S_n)$ ; diagonal subgroup of  $S_n \times S_n (\cong S_n)$

**Theorem** Let  $\Theta$  be an  $S_n \times S_n$ -primitive

$\Delta(S_n \times S_n)$ -invariant. For  $a, b \in K^r$ , assume that

(1)  $f_a^{S_n}(X)$  and  $f_b^{S_n}(X)$  are irreducible over  $K$ ;

(2)  $\text{Gal}_K f_a^{S_n}(X) \cong \text{Gal}_K f_b^{S_n}(X) =: G$

and all subgroups of  $G$  with index  $n$  are conjugate in  $G$ ;

(3)  $\mathcal{RP}_{\Theta, S_n \times S_n, f}(X)$  has no multiple root.

Then

$$L_a = L_b \iff \mathcal{RP}_{\Theta, S_n \times S_n, f}(X) \text{ has a root in } K$$

**The case of  $f_s^{S_3}(X) = X^3 + sX + s$**

$$f = f_s^{S_3}(X) f_t^{S_3}(X)$$

**Take  $\Theta = x_1y_1 + x_2y_2 + x_3y_3$  then we obtain**

$$\begin{aligned} F_{s,t}(X) &:= \mathcal{RP}_{\Theta, S_n \times S_n, f}(X) \\ &= X^6 - 6stX^4 - 27stX^3 + 9s^2t^2X^2 \\ &\quad + 81s^2t^2X - s^2t^2(4st + 27s + 27t) \end{aligned}$$

**For  $a, b \in K$ ,**

$$L_a = L_b \iff F_{a,b}(X) \text{ has a root in } K$$

**Moreover we get an answer of the **field intersection** problem:**

**Thm. (Field intersection problem**

$$\text{of } f_s^{S_3}(X) = X^3 + sX + s)$$

For  $a \in K$ , put  $L_a := \text{Spl}_K f_a^{S_3}(X)$ ,  $G_a := \text{Gal}(L_a/K)$

Assume  $C_3 \leq G_a \leq G_b$  and  $F_{a,b}(X)$  has no multiple root

$(G_a, G_b)$		decom. $F_{a,b}(X)$
$(S_3, S_3)$	$L_a \cap L_b = K$	6
	$[L_a \cap L_b : K] = 2$	3, 3
	$L_a = L_b$	3, 2, 1
$(C_3, S_3)$	$L_a \cap L_b = K$	6
$(C_3, C_3)$	$L_a \neq L_b$	3, 3
	$L_a = L_b$	3, 1, 1, 1

**Idea of the proof : formal Tschirnhausen transformation**

$f(X) \in K[X]$ : monic, degree  $n$ ,

roots  $\alpha_1, \dots, \alpha_n$  in fixed alg. closure of  $K$

$g(X)$  is Tschirnhausen transformation of  $f(X)$  over  $K$

$$\stackrel{\text{def}}{\iff} \exists c_0, \dots, c_{n-1} \in K$$

$$\text{s.t. } g(X) = \prod_{i=1}^n \left( X - \sum_{j=0}^{n-1} c_j \alpha_i^j \right)$$

$f(X) \sim_K g(X)$  : Tschirnhausen equivalent

$\stackrel{\text{def}}{\iff}$   $f(X)$  and  $g(X)$  are Tschirnhausen transformation each other

- $f(X), g(X) \in K[X]$ ; irreducible separable, degree  $n$

Roots  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$

$$f(X) \sim_K g(X)$$

$$\iff K(\alpha_i) = K(\beta_j) \text{ for some } i, j$$

$$\iff K[X]/(f(X)) \cong_K K[X]/(g(X))$$

- In particular,

$$f(X) \sim_K g(X) \implies \text{Spl}_K f(X) = \text{Spl}_K g(X)$$

- We consider **formal** Tschirnhausen transformation as follows:

- We consider a Tschirnhausen transformation

$$f_s(X) = \prod_{i=1}^n (X - x_i) \longrightarrow f_t(X) = \prod_{i=1}^n (X - y_i)$$

$$y_i = u_0 + u_1 x_i + \cdots + u_{n-1} x_i^{n-1}, \quad (i = 1, \dots, n)$$

Then we see

$$\begin{bmatrix} u_0(\overline{x}, \overline{y}) \\ u_1(\overline{x}, \overline{y}) \\ \vdots \\ u_{n-1}(\overline{x}, \overline{y}) \end{bmatrix} = D^{-1} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

where  $D = [x_i^{j-1}]_{1 \leq i, j \leq n}$  ; the Vandermonde matrix

**By Cramer's rule,**

$$u_i(\vec{x}, \vec{y}) = \Delta_{\mathbf{x}}^{-1} \cdot \det \begin{bmatrix} 1 & x_1 & \cdots & x_1^{i-1} & y_1 & x_1^{i+1} & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{i-1} & y_2 & x_2^{i+1} & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{i-1} & y_n & x_n^{i+1} & \cdots & x_n^{n-1} \end{bmatrix}$$

where  $\Delta_{\mathbf{x}} := \prod_{1 \leq i < j \leq n} (x_j - x_i)$

**Write  $u_i := u_i(\vec{x}, \vec{y})$ , ( $i = 0, \dots, n - 1$ ) for simplicity**

**Key Lemma**  $u_i \in K(x_1, \dots, x_n, y_1, \dots, y_n)$  is  
 $S_n \times S_n$ -primitive  $\Delta(S_n \times S_n)$ -invariant

**The case of  $S_3$  :  $f_s^{S_3}(X) = X^3 + sX + s$**

**Take  $\Theta = u_i, (i = 0, 1, 2),$  (formal Tschirn.-coeff.)**

$$G = S_n \times S_n, H = \Delta(S_n \times S_n),$$

$$f = f_s^{S_3} f_t^{S_3}, \text{ where } f_s^{S_3} = X^3 + sX + s$$

**We obtain  $G$ -relative  $H$ -invariant resolvent of  $f$  by  $\Theta = u_i$**

$$F_{s,t}^i(X) := \mathcal{RP}_{u_i, G, f}(X) = \prod_{\bar{\pi} \in G/H} (X - \omega_f(\pi(u_i)))$$

$$(i = 0, 1, 2)$$

**For  $a, b \in K,$**

$$L_a = L_b \iff F_{a,b}^i(X) \text{ has a root in } K$$

We see

$$F_{s,t}^0(X) = X^6 - \frac{8s^3t}{D_s}X^4 - \frac{8s^3t}{D_s}X^3 + \frac{16s^6t^2}{D_s^2}X^2 + \frac{32s^6t^2}{D_s^2}X - \frac{64s^8t^2(s-t)}{D_s^3},$$

$$F_{s,t}^1(X) = X^6 + \frac{6s^2t}{D_s}X^4 + \frac{27st}{D_s}X^3 + \frac{9s^4t^2}{D_s^2}X^2 + \frac{81s^3t^2}{D_s^2}X + \frac{s^4t^2(27s^2 + 729t + 108st + 4s^2t)}{D_s^3},$$

$$F_{s,t}^2(X) = X^6 - \frac{18st}{D_s}X^4 - \frac{27t}{D_s}X^3 + \frac{81s^2t^2}{D_s^2}X^2 + \frac{243st^2}{D_s^2}X - \frac{729s^2t^2(s-t)}{D_s^3}$$

where  $D_s = -s^2(4s + 27)$  (discriminant of  $X^3 + sX + s$ )

Finally we put  $u := 3 \cdot u_1 / u_2$

then we get

$$\begin{aligned} F_{s,t}(X) &= (s - t) \cdot \mathcal{RP}_{u,G,f}(X) \\ &= s(X^2 + 9X - 3s)^3 - t(X^3 - 2sX^2 - 9sX - 2s^2 - 27s)^2; \end{aligned}$$

$G$ -relative  $H$ -invariant resolvent of  $f$  by  $u$

$$(G = S_n \times S_n, H = \Delta(S_n \times S_n), f = f_s^{S_3} f_t^{S_3})$$

For  $a, b \in K$ ,

$$L_a = L_b \iff F_{a,b}(X) \text{ has a root in } K$$

This resolvent is **linear** in  $t$  !  $\longrightarrow$  **Thm. 1**

$$(t \longleftrightarrow b, \quad s \longleftrightarrow a, \quad X \longleftrightarrow u)$$

**Thm. 1 (H. - Miyake)** Assume that  $\text{char } k \neq 3$ .

Let  $f_s^{S_3}(X) := X^3 + sX + s \in k(s)[X]$ .

For  $a, b \in K$ ,  $\text{Spl}_K f_a^{S_3}(X) = \text{Spl}_K f_b^{S_3}(X)$

$\iff \exists u \in K$  s.t.

$$b = \frac{a(u^2 + 9u - 3a)^3}{(u^3 - 2au^2 - 9au - 2a^2 - 27a)^2}$$

By the similar way, we get

**Thm. 2 (H. - Miyake)** Assume that  $\text{char } k \neq 2$ .

Let  $f_t^{C_3}(X) := X^3 - tX^2 - (t + 3)X - 1 \in k(t)[X]$ .

For  $m, n \in K$ ,  $\text{Spl}_K f_m^{C_3}(X) = \text{Spl}_K f_n^{C_3}(X)$

$$\iff \exists z \in K \text{ s.t. either } n = \frac{m(z^3 - 3z - 1) - 9z(z + 1)}{mz(z + 1) + z^3 + 3z^2 - 1}$$

$$\text{or } n = -\frac{m(z^3 + 3z^2 - 1) + 3(z^3 - 3z - 1)}{mz(z + 1) + z^3 + 3z^2 - 1}$$

§4 Application of the results:  
 a parametrized family of cubic Thue equations

Take  $\underline{K} = \mathbb{Q}$  and **Shanks' simplest cubic**

$$f_m^{C_3}(X) = X^3 - mX^2 - (m+3)X - 1 \text{ for } \underline{m} \in \mathbb{Z}$$

$L_m := \text{Spl}_{\mathbb{Q}} f_m^{C_3}(X)$  is called simplest cubic fields

We consider a parametric family of cubic Thue equations

$$F_m(X, Y) := X^3 - mX^2Y - (m+3)XY^2 - Y^3 = j$$

for  $m \in \mathbb{Z}$  and  $j \in \mathbb{Z} \setminus \{0\}$ .

$$F_m(X, Y) := X^3 - mX^2Y - (m+3)XY^2 - Y^3 = j$$

- $j = \pm 1$ , Thomas (1990) (for  $m+1 \geq 1.365 \times 10^7$ ,  $m+1 \leq 10^3$ ) and Mignotte (1993) (the remaining case)

solved  $F_m(X, Y) = \pm 1$  completely

**Note that**

$$F_{-m-3}(X, Y) = F_m(-Y, -X),$$

$$-F_m(X, Y) = F_m(-X, -Y)$$

**Hence we can suppose that  $-1 \leq m$  and  $0 < j$  (WLOG)**

$$F_m(X, Y) := X^3 - mX^2Y - (m + 3)XY^2 - Y^3 = j$$

**For  $-1 \leq m \in \mathbb{Z}$  and  $j = 1$ , all integer solutions of**

**$F_m(X, Y) = 1$  are given by trivial solutions**

**$(x, y) = (0, -1), (-1, 1), (1, 0)$  for an arbitrary  $m$**

**and additionally**

$$(x, y) = (-1, -1), (-1, 2), (2, -1) \quad \text{for } m = -1,$$

$$(x, y) = (-9, 5), (5, 4), (4, -9) \quad \text{for } m = -1,$$

$$(x, y) = (-3, 2), (2, 1), (1, -3) \quad \text{for } m = 0,$$

$$(x, y) = (-7, -2), (-2, 9), (9, -7) \quad \text{for } m = 2$$

$$F_m(X, Y) := X^3 - mX^2Y - (m+3)XY^2 - Y^3 = j$$

- $F_m(X, Y)$  is invariant under  $X \mapsto Y \mapsto -X - Y$ ,
- $(x, y)$  is integer solution  
 $\implies (y, -x - y)$  and  $(-x - y, x)$  are also integer solutions
- Mignotte-Pethö-Lemmermeyer (1996) investigated  
 $F_m(X, Y) = j$  for general  $j \in \mathbb{Z}$   
 and gave a complete solution to Thue inequality  
 $|F_m(X, Y)| \leq 2m + 3$
- Lettl-Pethö-Voutier (1999) studied Thue inequality  
 $|F_m(X, Y)| \leq j(m)$  where  $j : \mathbb{Z} \rightarrow \mathbb{N}$   
under some assumption by the hypergeometric method

$$L_m := \text{Spl}_{\mathbb{Q}} f_m^{C_3}(X) \quad \bullet \quad \boxed{L_m = L_{-m-3} \text{ for } m \in \mathbb{Z}}$$

By **Thm. 2**,

$L_n = L_m \iff \exists z \in \mathbb{Q}$  s.t. either

$$n = \frac{m(z^3 - 3z - 1) - 9z(z+1)}{mz(z+1) + z^3 + 3z^2 - 1} \text{ or } n = -\frac{m(z^3 + 3z^2 - 1) + 3(z^3 - 3z - 1)}{mz(z+1) + z^3 + 3z^2 - 1}$$

Write  $z = y/x$  with  $\gcd(x, y) = 1$  then we have

$$n = m + \frac{(m^2 + 3m + 9)xy(x+y)}{F_m(x, y)} \text{ or } n = -m - 3 - \frac{(m^2 + 3m + 9)xy(x+y)}{F_m(x, y)}$$

• If  $\exists x, y \in \mathbb{Z}$  s.t.  $F_m(x, y) =: j \mid (m^2 + 3m + 9)$  and  $xy(x + y) \neq 0$  then  $\exists n \in \mathbb{Z} \setminus \{m, -m - 3\}$  s.t.  $L_n = L_m$

• we can show that **the converse also holds**, namely

**Thm. 3** For a given  $m \in \mathbb{Z}$ ,

$\exists n \in \mathbb{Z} \setminus \{m, -m - 3\}$  s.t.  $L_m = L_n$

$\implies \exists (x, y) \in \mathbb{Z}^2$  with  $xy(x + y) \neq 0$  s.t.

$$F_m(x, y) = j$$

for some  $j \in \mathbb{N}$  with  $j \mid (m^2 + 3m + 9)$ .

Conversely  $\exists$  such an integer solution  $(x, y) \in \mathbb{Z}^2$

$\implies n \in \mathbb{Z} \setminus \{m, -m - 3\}$  which satisfies

$L_n = L_m = L_{-m-3}$  is given as

$$n = m + \frac{(m^2 + 3m + 9)xy(x + y)}{F_m(x, y)}.$$

Hence we get

for a given  $m \in \mathbb{Z}$ ,

$$\exists n \in \mathbb{Z} \setminus \{m, -m - 3\} \text{ s.t. } L_n = L_m$$

$\Updownarrow$  **Thm. 3**

$$\begin{aligned} \exists (x, y) \in \mathbb{Z}^2 \text{ with } xy(x + y) \neq 0 \\ \text{s.t. } F_m(x, y) = j \mid m^2 + 3m + 9 \end{aligned}$$

Note that

- (i) the discriminant of  $F_m(X, Y)$  is  $(m^2 + 3m + 9)^2$ ,
- (ii) if  $xy(x + y) = 0$  then  $|F_m(x, y)| \in \mathbb{Z}^3$   
and hence for  $j \in \mathbb{Z}^3$  another trivial solutions exist

**R. Okazaki (2002) studied Thue equation  $f(X, Y) = 1$   
for an irreducible cubic form  $f(X, Y)$   
with positive discriminant**

**He established a strong result on gaps between solutions**

**For example**

**Take  $f(X, Y)$  as**

$$F_m(X, Y) = X^3 - mX^2Y - (m + 3)XY^2 - Y^3$$

**We get**

$$40000 \leq m + 1$$

**$\implies F_m(X, Y) = 1$  has only three trivial solutions**

$$(x, y) = (0, -1), (-1, 1), (1, 0)$$

Using this result, Okazaki showed the following theorem:

**Thm. (R. Okazaki)** For  $-1 \leq m, n \in \mathbb{Z}$ ,

if  $L_m = L_n$  ( $m \neq n$ ) then

$m, n \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ .

$$L_{-1} = L_5 = L_{12} = L_{1259},$$

$$L_0 = L_3 = L_{54},$$

$$L_1 = L_{66},$$

$$L_2 = L_{2389}$$

In particular, we get

Although the result seems to be unpublished yet (up to now),  
a brief sketch of the proof is available at

<http://www1.doshisha.ac.jp/~rokazaki/papers.html>

$$F_m(X, Y) := X^3 - mX^2Y - (m + 3)XY^2 - Y^3 = j$$

As a consequence of **Thm. 3** and Okazaki's Thm.,  
we obtain the following corollaries:

**Cor.** For  $m \geq -1$ , the all integer solutions  $(x, y) \in \mathbb{Z}^2$   
with  $xy(x + y) \neq 0$  of Thue equations  $F_m(X, Y) = j$   
with  $j \in \mathbb{N}$  and  $j \mid (m^2 + 3m + 9)$  are given on **Table 1**.

Table 1

$m$	$n$	$-n - 3$	$j$	$m^2 + 3m + 9$	$xy(x + y)$	$(x, y)$
-1	-15	12	1	7	-2	$(-1, -1), (-1, 2), (2, -1)$
-1	1259	-1262	1	7	180	$(-9, 5), (5, 4), (4, -9)$
-1	5	-8	7	7	6	$(-3, 2), (2, 1), (1, -3)$
0	54	-57	1	9	6	$(-3, 2), (2, 1), (1, -3)$
0	-6	3	3	9	-2	$(-1, -1), (-1, 2), (2, -1)$
1	-69	66	13	13	-70	$(-5, -2), (-2, 7), (7, -5)$
2	-2392	2389	1	19	-126	$(-7, -2), (-2, 9), (9, -7)$
3	-3	0	9	27	-2	$(-1, -1), (-1, 2), (2, -1)$
3	-57	54	9	27	-20	$(-4, -1), (-1, 5), (5, -4)$
5	1259	-1262	49	49	1254	$(-22, 19), (19, 3), (3, -22)$
5	-15	12	49	49	-20	$(-4, -1), (-1, 5), (5, -4)$
5	-1	-2	49	49	-2	$(-2, 3), (3, -1), (-1, -2)$
12	-2	-1	27	$3^3 \cdot 7$	-2	$(-1, -1), (-1, 2), (2, -1)$
12	-1262	1259	27	$3^3 \cdot 7$	-182	$(-13, -1), (-1, 14), (14, -13)$
12	-8	5	$3^3 \cdot 7$	$3^3 \cdot 7$	-20	$(-4, -1), (-1, 5), (5, -4)$
54	0	-3	$7^3$	$3^2 \cdot 7^3$	-6	$(-2, 3), (3, -1), (-1, -2)$
54	-6	3	$3 \cdot 7^3$	$3^2 \cdot 7^3$	-20	$(-4, -1), (-1, 5), (5, -4)$
66	-4	1	$3^3 \cdot 13^2$	$3^3 \cdot 13^2$	-70	$(-5, -2), (-2, 7), (7, -5)$
1259	-1	-2	$61^3$	$7 \cdot 61^3$	-180	$(-5, 9), (9, -4), (-4, -5)$
1259	-15	12	$61^3$	$7 \cdot 61^3$	-182	$(-13, -1), (-1, 14), (14, -13)$
1259	5	-8	$7 \cdot 61^3$	$7 \cdot 61^3$	-1254	$(-19, 22), (22, -3), (-3, -19)$
2389	-5	2	$67^3$	$19 \cdot 67^3$	-126	$(-7, -2), (-2, 9), (9, -7)$

$$F_m(X, Y) := X^3 - mX^2Y - (m + 3)XY^2 - Y^3 = j$$

**Cor.** For  $m \geq -1$ , integer solutions  $(x, y) \in \mathbb{Z}^2$   
with  $xy(x + y) \neq 0$  of Thue equations

$$F_m(X, Y) = m^2 + 3m + 9$$

exist only for  $m = -1, 1, 5, 12, 66, 1259$  as on Table 1.

## §5 Some numerical examples: the quintic case

Take a  $k$ -generic polynomial for  $D_5$  (Brumer's form) :

$$f_{s,t}^{D_5}(X) = X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2-t-2s-1)X^2 + sX + t$$

We obtained an **explicit formula** of two resolvent polynomials

$$F_{s,t,s',t'}^1(X), F_{s,t,s',t'}^2(X) \in k(s, t, s', t')[X] ; \text{degree } 10$$

**Thm. 4** For  $\mathbf{a} = (a_1, a_2), \mathbf{b} = (b_1, b_2) \in K^2$ ,

$$L_{\mathbf{a}} = L_{\mathbf{b}} \iff F_{\mathbf{a},\mathbf{b}}^1(X) \cdot F_{\mathbf{a},\mathbf{b}}^2(X) \text{ has a root in } K.$$

See, in detail, arXiv: 0804.4875v1 [math.NT]

Moreover we get an answer of the **field intersection** problem:

**Thm. (Field intersection problem of  $f_{s,t}^{D_5}$ )**

For  $\mathbf{a} = (a_1, a_2), \mathbf{b} = (b_1, b_2) \in K^2,$

put  $G_{\mathbf{a}} := \text{Gal}_K f_{a_1, a_2}^{D_5}(X), \quad G_{\mathbf{b}} := \text{Gal}_K f_{b_1, b_2}^{D_5}(X)$

Assume  $G_{\mathbf{a}} \geq G_{\mathbf{b}} \geq C_5$  then we have:

$G_{\mathbf{a}}$	$G_{\mathbf{b}}$			decom. $F_{\mathbf{a}, \mathbf{b}}^1$	decom. $F_{\mathbf{a}, \mathbf{b}}^2$	
$D_5$	$D_5$	$D_5 \times D_5$	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	10	10	
		$(C_5 \times C_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{b}} : K] = 2$	5, 5	5, 5	
		$D_5$	$L_{\mathbf{a}} = L_{\mathbf{b}}$	5, 2, 2, 1	5, 5	
	$C_5$	$C_5$	$D_5 \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	5, 5	5, 2, 2, 1
			$D_5 \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{b}} = K$	10	10
$C_5$	$C_5$	$C_5 \times C_5$	$L_{\mathbf{a}} \neq L_{\mathbf{b}}$	5, 5	5, 5	
		$C_5$	$C_5$	$L_{\mathbf{a}} = L_{\mathbf{b}}$	5, 1 <sup>5</sup>	5, 5
	$L_{\mathbf{a}} = L_{\mathbf{b}}$			5, 5	5, 1 <sup>5</sup>	

**Example 1** Take  $K = \mathbb{Q}$  and  $t := 1$ . Then

$$f_{s,1}^{D_5}(X) = X^5 - 2X^4 + (s+2)X^3 - (2s+1)X^2 + sX + 1$$

For  $a_1, b_1 \in \mathbb{Z}$  in the range  $-10000 \leq a_1 < b_1 \leq 10000$ ,

$$\text{Spl}_{\mathbb{Q}} f_{a_1,1}^{D_5}(X) = \text{Spl}_{\mathbb{Q}} f_{b_1,1}^{D_5}(X)$$

$\iff (a_1, b_1) \in X_1 \cup X_2$  where

$$X_1 = \{(-6, 0), (-1, 41), (-94, -10)\},$$

$$X_2 = \{(-1, 0), (-6, -1), (-18, -7),$$

$$(1, 34), (0, 41), (-6, 41), (-167, -8)\}$$

For each  $i = 1, 2$ , we checked by **Thm. 4** that

$$(a_1, b_1) \in X_i \iff F_{a_1,1,b_1,1}^i(X) \text{ has a root in } \mathbb{Q}$$

for  $-10000 \leq a_1 < b_1 \leq 10000$

**Example 2** Take  $K = \mathbb{Q}$ .

**Kida-Renault-Yokoyama (to appear in Int. J. Number Theory) showed that**

$$\exists \infty b_1 \in \mathbb{Q} \text{ s.t. } \text{Spl}_{\mathbb{Q}} f_{0,1}^{D_5}(X) = \text{Spl}_{\mathbb{Q}} f_{b_1,1}^{D_5}(X).$$

**Their method enables us to construct such  $b_1$ 's explicitly via rational points of the associated elliptic curve.**

**They also pointed out that in the range**

$$-400 \leq b_1, b_2 \leq 400,$$

$$\exists 25 \text{ pairs } (b_1, b_2) \in \mathbb{Z}^2 \text{ s.t. } \text{Spl}_{\mathbb{Q}} f_{0,1}^{D_5}(X) = \text{Spl}_{\mathbb{Q}} f_{b_1,b_2}^{D_5}(X)$$

We can classify the 25 pairs by **Thm. 4**;

$$\mathbf{Spl}_{\mathbb{Q}} f_{0,1}^{D_5}(X) = \mathbf{Spl}_{\mathbb{Q}} f_{b_1,b_2}^{D_5}(X)$$

$$\iff F_{0,1,b_1,b_2}^i(X), (i = 1, 2) \text{ has a root in } \mathbb{Q}$$

$$\iff (b_1, b_2) \in X_i, (i = 1, 2) \text{ where}$$

$$X_1 = \{(0, 1), (4, -1), (4, 5), (-6, 1), (-24, 19), (34, 11), (36, -5), \\ (46, -1), (-188, 23), (264, 31), (372, -5), (378, 43)\},$$

$$X_2 = \{(-1, -1), (-1, 1), (5, -1), (41, 1), (-43, 5), (47, 13), (59, -5), \\ (59, 19), (101, 19), (125, -23), (149, 11), (155, 25), (-169, 55)\}$$

By **Thm. 4**, we can show that

$$F_{0,1,b_1,b_2}^1(X) \text{ has a root in } \mathbb{Q} \implies (b_1, b_2) = (\text{even}, \text{odd})$$

$$F_{0,1,b_1,b_2}^2(X) \text{ has a root in } \mathbb{Q} \implies (b_1, b_2) = (\text{odd}, \text{odd})$$

**We do not know, however, whether  $\exists \infty (s_1, t_1) \in \mathbb{Z}^2$   
s.t.  $\text{Spl}_{\mathbb{Q}} f_{0,1}^{D_5}(X) = \text{Spl}_{\mathbb{Q}} f_{b_1,b_2}^{D_5}(X)$  or not**

**By [Thm. 4](#) (an explicit formula), we checked such pairs  
in the range  $-20000 \leq b_1, b_2 \leq 20000$ ;**

**and we should add just**

$$X_1 = \{(526, 41), (952, 113), (2302, 95), \\ (6466, 311), (7180, 143), (7480, -169)\}$$

$$X_2 = \{(785, -25), (3881, 29), (-11215, 299), (19739, -281)\}$$

**Example 3** Let  $h_n(X)$  be Lehmer's simplest quintic

$$h_n(X) = X^5 + n^2 X^4 - (2n^3 + 6n^2 + 10n + 10)X^3 \\ + (n^4 + 5n^3 + 11n^2 + 15n + 5)X^2 + (n^3 + 4n^2 + 10n + 10)X + 1$$

and take  $K = \mathbb{Q}(\text{Gal}(h_n(X)/\mathbb{Q}) = C_5)$

For Brumer's quintic  $f_{s,t}^{D_5}(X)$ , we see that

$\text{Spl}_{\mathbb{Q}(n)} h_n(X) = \text{Spl}_{\mathbb{Q}(n)} f_{s,t}^{D_5}(X)$  where

$$s = -20 - 5n + 10n^2 + 12n^3 + 5n^4 + n^5,$$

$$t = -7 - 10n - 5n^2 - n^3$$

Using **Thm. 4**, we checked pairs  $(n, m) \in \mathbb{Z}^2$  in the range

$-10000 \leq n < m \leq 10000$  to confirm that

$$\text{Spl}_{\mathbb{Q}} h_n(X) = \text{Spl}_{\mathbb{Q}} h_m(X) \iff (n, m) = (-2, -1)$$

**Thm. 4** For  $\mathbf{a} = (a_1, a_2)$ ,  $\mathbf{b} = (b_1, b_2) \in K^2$ ,

$L_{\mathbf{a}} = L_{\mathbf{b}} \iff F_{\mathbf{a},\mathbf{b}}^1(X) \cdot F_{\mathbf{a},\mathbf{b}}^2(X)$  has a root in  $K$

where

$$F_{s,s'}^1(X) := \left( X^5 - (t-3)(t'-3)X^4 + c_3X^3 + \frac{c_2}{2}X^2 + \frac{c_1}{2}X + \frac{c_0}{2} \right)^2 - \frac{d^2 d'^2}{4} \left( X^2 + (t+t'-1)X + (s-t+s'-t'+tt'+2) \right)^2,$$

$$F_{s,s'}^2(X) := F_{(s+5t)/t^2, -1/t, s', t'}^1(X)$$

and  $d^2 \in k(s, t)$  is given by

$$d^2 = s^2 - 4s^3 + 4t - 14st - 30s^2t - 91t^2 - 34st^2 + s^2t^2 + 40t^3 + 24st^3 + 4t^4 - 4t^5$$

The coefficients  $c_3, c_2, c_1, c_0 \in k(s, t, s', t')$  of  $F_{s,s'}^1(X)$  are explicitly given in terms of  $\mathbf{s} = (s, t)$  and  $\mathbf{s}' = (s', t')$  as

$$c_3 = \left[ 2s - 21t + 3t^2 - 2ts' + t^2s' - t^2t' \right] + 31 - 3ss' + 5tt',$$

$$c_2 = \left[ -20s + 112t + 8st - 32t^2 + 2t^3 + 5ts' - 13sts' - 12t^2s' + 4t^3s' - 15stt' \right. \\ \left. + 14t^2t' + 2t^3t' + 8t^2s't' - 2t^3t'^2 \right] - 102 + 27ss' - 119tt' - sts't' + 6t^2t'^2,$$

$$c_1 = \left[ 32s + 2s^2 - 128t - 26st + 60t^2 + 4st^2 - 8t^3 - 6s^2s' - 7ts' + 38sts' + 9t^2s' - 5st^2s' \right. \\ \left. - 12t^3s' + 2t^4s' - 20ts'^2 - 8sts'^2 + 6t^2s'^2 + 2t^3s'^2 + 2stt' - 77t^2t' + 3st^2t' + 8t^3t' - 29t^2s't' \right. \\ \left. + st^2s't' + 18t^3s't' - 2st^2t'^2 + 10t^3t'^2 \right] + 80 - 37ss' + 145tt' - 45sts't' + 24t^2t'^2 - 8t^3t'^3,$$

$$c_0 = \left[ -16s - 2s^2 + 56t + 24st + 2s^2t - 38t^2 - 8st^2 + 8t^3 + 5s^2s' - 2ts' - 38sts' - 7s^2ts' \right. \\ \left. + 5t^2s' + 13st^2s' + 8t^3s' + 2st^3s' - 4t^4s' - 21ts'^2 - 11sts'^2 - 2t^2s'^2 + 2st^2s'^2 + 4t^3s'^2 \right. \\ \left. - 104stt' - 33s^2tt' + 105t^2t' + 35st^2t' + 4t^3t' + 16st^3t' - 6t^4t' - 2t^5t' - s^2ts't' + 36t^2s't' \right. \\ \left. - 14st^2s't' - 6t^3s't' + 6t^4s't' + 8t^2s'^2t' - 37st^2t'^2 + 22t^3t'^2 - 2st^3t'^2 + 8t^4t'^2 + 8t^3s't'^2 \right. \\ \left. - 2t^4t'^3 \right] - 24 + 14ss' - 8s^2s'^2 - 224tt' + sts't' - 101t^2t'^2 - st^2s't'^2 - 8t^3t'^3$$

where  $[a] := a + \iota(a)$

with  $\iota : s \leftrightarrow s', t \leftrightarrow t'$  for  $a \in k(s, t, s', t')$