Invariants and hyperelliptic curves: algorithmic aspects and open questions

R. Lercier, C. Ritzenthaler and Jeroen Sijsling

IML - CNRS (Marseille)

Trento, Sep. 2012

The genus 1 case

Let K be an algebraically closed field of characteristic $p \neq 2$.

- Elliptic curves $(p \neq 3)$ $E/K \; : y^2 = x^3 + a\,x + b$ are classified up to isomorphism by

$$j(E) = 1728\,\frac{4a^3}{4\,a^3 + 27\,b^2}\,.$$

- Conversely, for any $j \in K \setminus \{1728\}$, we can reconstruct a curve E s.t. $j(E) = j$, for instance

$$E/K : y^2 = x^3 - \frac{27\,j}{j - 1728}\,x + \frac{54\,j}{j - 1728}\,.$$

- Similarly, we would like to do the same for hyperelliptic curves of genus $g \geq 2$, *i.e.* $C/K : y^2 = f(x)$ with $\deg(f) = 2g + 2$ and simple roots.

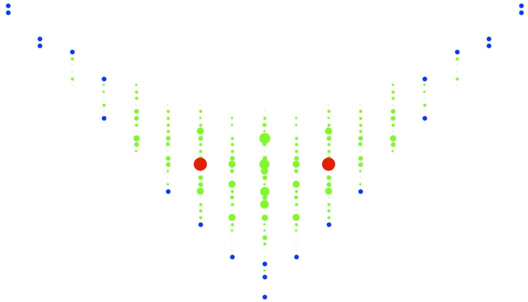
$$\{\text{Hyperelliptic curves of genus } g\}_{/\simeq} \;\longleftrightarrow\; \{\text{a `space' of parameters}\}$$

Concretely for $g = 3$...(Lercier-R. 2012)

```
> _<x> := PolynomialRing(GF(11));
> H1 := HyperellipticCurve(7*x^8 + 5*x^6 + 5*x^4 + 3*x^2 + x + 9);

> ShiodaInvariants(H1);
[ 8, 2, 4, 10, 2, 7, 8, 9, 3 ]

> H2, G := HyperellipticCurveFromShiodaInvariants($1); H2;
Hyperelliptic Curve defined by
  y^2 = x^8 + x^7 + x^6 + 4*x^5 + x^4 + x^2 + 5*x + 8 over GF(11)

> IsIsomorphic(H1, H2);
true
> IdentifyGroup(G);
<8, 5>
```

Why do we want do be able to do this ?

- check if two curves are isomorphic;
- recognize quickly the group of automorphisms;
- geometric and arithmetic information about the moduli space;
- construction of curves with special properties (CM structure,. . .);
- enumeration of curves over finite fields for experiments.



Distribution of genus 2 curves over $\mathbb{F}_7$ among isogeny classes

Isomorphisms

Proposition

Let $C : y^2 = f(x)$ $C : y^2 z^{2g-2} = f(x, z)$ *and* $C' : y^2 = f'(x)$ $C' : y^2 z^{2g-2} = f'(x, z)$ *be two hyperelliptic curves of genus* g*. Every isomorphism from* C *to* C' *is of the form*

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^{g+1}} \right),$$

$$(x, z, y) \mapsto (ax + bz, cx + dz, ey)$$

for some $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(K)$ *and* $e \in K^*$*.*

This reduces the question to invariants of degree $2g + 2$ binary forms under $\mathrm{GL}_2(K)$.

From curves to invariants

Fact: the algebra of invariants $\mathcal{I}_n$ is finitely generated (Gordan 1868) and for $n \leq 10$ (and $12, 14, 16$ (Lercier, unpublished)) generators are explicitly known in characteristic 0.[1]

Ex: $n = 4$, $f = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. There is one covariant of degree 2 and order 4

$$(f,f)_2 = (1/3a_2a_4 - 1/8a_3^2)x^4 + (a_1a_4 - 1/6a_2a_3)x^3 + (2a_0a_4 + 1/4a_1a_3 - 1/6a_2^2)x^2 + (a_0a_3 - 1/6a_1a_2)x + 1/3a_0a_2 - 1/8a_1^2.$$

The algebra of invariants $\mathcal{I}_4$ is generated by

$$I = (f,f)_4 = 2a_0a_4 - 1/2a_1a_3 + 1/6a_2^2$$

and by

$$J = (f,(f,f)_2)_4 = a_0a_2a_4 - 3/8a_0a_3^2 - 3/8a_1^2a_4 + 1/8a_1a_2a_3 - 1/36a_2^3.$$

Rem. The j-invariant is equal to $1728I^3/(I^3 - 6J^2)$.

[1] Shioda's computation for $n = 8$ *are* correct up to two typos.

What about characteristic $\neq 0$?

(Geyer 1974) proved that reduction of $\mathcal{I}_n$ modulo p works well when $p > n$.

Q.1: is there a way to adapt Gordan's algorithm to generate invariants valid in all characteristics $> n$?

Q.2: what can be done in small characteristics? (solved for genus 2 and work in progress for $g = 3$ by Basson – for instance in characteristic 5 for binary octics, there is a invariant of degree 1).

Q.3: what about genus 3 non hyperelliptic curves (=smooth plane quartics)? Primary invariants by (Dixmier 1987) and a complete set of generators by (Ohno 2004).

From invariants to curves

- Starting from a 'list' $(j_1 : j_2 : \ldots)$ of values of $J_i(f)$ in K, we aim at recovering a hyperelliptic curve C/K, isomorphic to $y^2 = f(x)$.
- In general, inverting the polynomial system giving the invariants in terms of a generic polynomial $f = \sum_i a_i x^i$ is quickly impossible.

$$J_2 = 2\, a_0\, a_8 - \frac{1}{4}\, a_1\, a_7 + \frac{1}{14}\, a_2\, a_6 - \frac{1}{28}\, a_3\, a_5 + \frac{1}{70}\, {a_4}^2,$$
$$J_3 = \frac{3}{35}\, a_0\, a_4\, a_8 - \frac{3}{56}\, a_0\, a_5\, a_7 + \frac{9}{392}\, a_0\, {a_6}^2 - \frac{3}{56}\, a_1\, a_3\, a_8 + \frac{9}{560}\, a_1\, a_4\, a_7 - \frac{3}{784}\, a_1\, a_5\, a_6 + \frac{9}{392}\, {a_2}^2 a_8 - \frac{3}{784}\, a_2\, a_3\, a_7 - \frac{33}{13720}\, a_2\, a_4\, a_6 + \frac{9}{5488}\, a_2\, {a_5}^2 + \frac{9}{5488}\, {a_3}^2 a_6 - \frac{27}{27440}\, a_3\, a_4\, a_5 + \frac{9}{34300}\, {a_4}^3,$$
$$J_4 = \cdots$$

- However, (Mestre 1991) suggested a general strategy based on nice formulae due to (Clebsch 1872).

Useful identities for three quadratic forms

Let q_1, q_2, q_3 be three binary homogeneous quadratic forms over K.

- The (quadratic) forms

$$q_1^* = (q_2, q_3)_1, \;\; q_2^* = (q_3, q_1)_1, \;\; q_3^* = (q_1, q_2)_1$$

  satisfy

$$q_1 q_1^* + q_2 q_2^* + q_3 q_3^* = 0 \text{ and } \sum_{i,j} A_{ij} q_i^* q_j^* = 0 \text{ where } A_{ij} = (q_i, q_j)_2 \,.$$

- Let R be the determinant of the q_i's in the basis x^2, xz, z^2. If f is a binary form of even degree n, then

$$R(q_1, q_2, q_3)^{n/2} \cdot f(X, Z) = \frac{1}{n!} \cdot \left(\sum_{i=1}^{3} q_i^*(X, Z) \delta_i \right)^{n/2} f(X_1, Z_1)$$

  (where δ_i is the differential operator $\phi(X_1, Z_1) \mapsto \Omega_{12}^2(\phi(X_1, Z_1) \cdot q_i(X_2, Z_2))$).

Generic reconstruction

1. Choose 3 covariants q_1, q_2, q_3 of order 2;

2. Construct from them a conic $\mathcal{Q} : \sum A_{ij} \cdot x_i x_j = 0$ and a plane degree $g+1$ curve $\mathcal{H} : \sum h_I \cdot x_I = 0$ satisfying

   - A_{ij} and h_I are invariants;
   - The point $(q_1^* : q_2^* : q_3^*)$ is solution of

$$\begin{cases} \sum A_{ij} \cdot q_i^* q_j^* = 0, \\ \sum h_I \cdot q_I^* - R(q_1, q_2, q_3)^{n/2} \cdot f(x,z) = 0, \end{cases}$$

   where $R(q_1, q_2, q_3)$ is zero iff the conic $\mathcal{Q}$ is singular.

3. After parametrization of $\mathcal{Q}$, the intersection points of $\mathcal{Q}$ and $\mathcal{H}$ are $\mathrm{GL}_2(K)$-equivalent to the zeros of f.

14 fundamental covariants of order 2 for octics

Ord. / Deg.	0	2	4	6	8	10	12	14	18	Tot
1	–	–	–	–	f	–	–	–	–	1
2	$(f, f)_8$	–	$(f, f)_6$	–	$(f, f)_4$	–	$(f, f)_2$	–	–	4
3	$(C_{2,8}, f)_8$	–	$(C_{2,8}, f)_6$	$(C_{2,8}, f)_5$	$(C_{2,8}, f)_4$	$(C_{2,8}, f)_3$	$(C_{2,8}, f)_2$	$(C_{2,8}, f)_1$	$(C_{2,12}, f)_1$	8
4	$(C_{3,8}, f)_8$	–	$(C_{3,4}, f)_4$ $(C_{3,8}, f)_6$	$(C_{3,4}, f)_3$	$(C_{3,4}, f)_2$	$(C_{3,4}, f)_1$ $(C_{3,8}, f)_3$	$(C_{3,8}, f)_2$	$(C_{3,8}, f)_1$	$(C_{3,12}, f)_1$	10
5	$(C_{4,8}, f)_8$	$(C_{4,10}, f)_8$	$(C_{4,10}, f)_7$ $(C_{4,8}, f)_6$	$(C_{4,10}, f)_6$ $(C_{4,8}, f)_5$	$(C_{4,10}, f)_5$	$(C_{4,8}, f)_3$ $(C_{4,10}, f)_4$ $(C'_{4,10}, f)_4$	–	$(C_{4,10}, f)_2$	–	11
6	$(C_{3,4}\, C_{2,4}, f)_8$	$(C_{5,8}, f)_7$	$(C_{5,8}, f)_6$ $(C'_{5,4}, f)_4$	$(C_{5,8}, f)_5$ $(C'_{5,4}, f)_3$ $(C'_{5,10}, f)_6$	$(C'_{5,4}, f)_2$	$(C'_{5,4}, f)_1$	–	–	–	9
7	$(C_{2,4}\, C'_{4,4}, f)_8$	$(C_{2,4}\, C_{4,6}, f)_8$ $(C''_{6,6}, f)_6$	$(C_{2,4}\, C_{4,6}, f)_7$ $(C''_{6,6}, f)_5$	$(C''_{6,6}, f)_4$ $(C_{6,2}, f)_2$ $(C_{2,4}\, C_{4,6}, f)_6$	–	–	–	–	–	8
8	$(C_{3,4}\, C_{4,4}, f)_8$	$(C_{2,8}\, C_{5,2}, f)_8$ $(C_{3,6}\, C_{4,4}, f)_8$	$(C_{3,6}\, C_{4,4}, f)_7$ $(C_{3,4}\, C_{4,6}, f)_7$	$(C_{3,6}\, C_{4,4}, f)_6$ $(C_{3,4}\, C_{4,6}, f)_6$	–	–	–	–	–	7
9	$(C_{2,4}\, C_{6,4}, f)_8$	$(C_{4,6}\, C'_{4,4}, f)_8$ $(C_{2,4}\, C_{6,4}, f)_7$ $(C_{2,4}\, C'_{6,6}, f)_8$	$(C_{2,4}\, C_{6,4}, f)_6$	–	–	–	–	–	–	5
10	$(C_{4,4}\, C'_{5,4}, f)_8$	$(C'_{7,2}\, C_{2,4}, f)_6$ $(C_{4,6}\, C_{5,4}, f)_8$	–	–	–	–	–	–	–	3
11	–	$(C'_{8,4}\, C_{2,4}, f)_7$ $(C'_{5,6}\, C'_{5,4}, f)_8$	–	–	–	–	–	–	–	2
12	–	$(C'_{6,6}\, C'_{5,4}, f)_8$	–	–	–	–	–	–	–	1
Tot	9	14	13	12	6	7	3	3	2	69

Table: Fundamental invariants and covariants for a binary homogeneous form $f(x, z)$ of degree 8

Example for $g = 3$

Choose $q_1 = C_{5,2}$, $q_2 = C_{6,2}$ and $q_3 = C_{7,2}$ (one among 364 choices).

$R(q_1, q_2, q_3)$ is the determinant of the q_i's in the basis x^2, xz, z^2.

$$
\begin{aligned}
R(q_1, q_2, q_3) = {} & -4937630140800 J_9^2 + 6172588800000 J_8 J_{10} + 1016336160000 J_6^3 - 1646487542700 J_5 J_6 J_7 + 475344450 J_5^2 J_8 \\
& - 13778100 J_4 J_7^2 + 6154254741600 J_4 J_6 J_8 + 2469123699840 J_4 J_5 J_9 - 3175414824960 J_4^2 J_{10} \\
& - 1028718873000 J_3 J_7 J_8 - 1555231104000 J_3 J_6 J_9 + 514676332800 J_3 J_5 J_{10} - 579162433500 J_2 J_8^2 \\
& + 231655788000 J_2 J_7 J_9 + 47632860 J_4^2 J_5^2 - 201602675520 J_4^3 J_6 - 264617457390 J_3 J_4 J_5 J_6 \\
& + 529262244990 J_3 J_4^2 J_7 + 4618063800 J_3^2 J_6^2 - 35210700 J_3^2 J_5 J_7 - 228766979700 J_3^2 J_4 J_8 \\
& + 38124172800 J_3^3 J_9 + 77149935135 J_2 J_5^2 J_6 - 40603006080 J_2 J_4 J_6^2 - 115812049185 J_2 J_4 J_5 J_7 \\
& - 330859026540 J_2 J_4^2 J_8 + 145802916000 J_2 J_3 J_6 J_7 - 15715198800 J_2 J_3 J_4 J_9 + 42877447200 J_2 J_3^2 J_{10} \\
& + 53596043550 J_2^2 J_7^2 - 145802916000 J_2^2 J_6 J_8 - 53606606760 J_2^2 J_5 J_9 + 137217628800 J_2^2 J_4 J_{10} \\
& - 36737464140 J_3^2 J_4^3 - 7824600 J_3^3 J_4 J_5 + 11300902200 J_3^4 J_6 - 47249726760 J_2 J_4^4 \\
& - 12161979900 J_2 J_3 J_4^2 J_5 + 33446455740 J_2 J_3^2 J_4 J_6 + 1760535 J_2^2 J_4 J_5^2 + 25514097660 J_2^2 J_4^2 J_6 \\
& - 153935460 J_2^3 J_6^2 + 1173690 J_2^3 J_5 J_7 + 7625565990 J_2^3 J_4 J_8 - 1270805760 J_2^3 J_3 J_9 - 1429248240 J_2^4 J_{10} \\
& + 289800 J_2 J_3^4 J_4 + 900887400 J_2^2 J_3^2 J_4^2 + 2575261188 J_2^3 J_4^3 + 260820 J_2^3 J_3 J_4 J_5 - 753393480 J_2^3 J_3^2 J_6 \\
& - 1114881858 J_2^4 J_4 J_6 - 19320 J_2^4 J_3^2 J_4 - 30029580 J_2^5 J_4^2 + 12556558 J_2^6 J_6 + 322 J_2^7 J_4 .
\end{aligned}
$$

Example (cont.)

$$
\begin{aligned}
\mathcal{Q} \;:\; 0 = {} & (9217732608000 J_{10} - 1422489600 J_2{}^3 J_4 + 1814283878400 J_4 J_6 - 384072192000 J_3 J_7 + 42674688000 J_3{}^2 J_4 \\
& - 1152216576000 J_5{}^2 + 212154163200 J_2 J_4{}^2 + 384072192000 J_2 J_8)\, x_1^{*\,2} \\
& + (-80015040000 J_3{}^2 J_5 + 2667168000 J_2{}^3 J_5 - 12002256000 J_2{}^2 J_7 + 288054144000 J_2 J_9 + 216040608000 J_4 J_7 \\
& - 102019176000 J_2 J_4 J_5 + 138883248000 J_3 J_4{}^2 - 48009024000 J_5 J_6 + 360067680000 J_3 J_8)\, x_1^* x_2^* \\
& + (-12040358400 J_2{}^2 J_8 - 902039040 J_2{}^3 J_6 - 24768737280 J_4{}^3 + 27061171200 J_3{}^2 J_6 + 18627840 J_2{}^4 J_4 \\
& - 424308326400 J_2 J_{10} - 5482391040 J_2{}^2 J_4{}^2 - 43481733120 J_2 J_4 J_6 + 216726451200 J_5 J_7 + 12040358400 J_2 J_3 J_7 \\
& - 762657638400 J_4 J_8 + 36121075200 J_2 J_5{}^2 + 135339724800 J_3 J_9 - 162570240000 J_6{}^2 - 10516262400 J_3 J_4 J_5 \\
& - 558835200 J_2 J_3{}^2 J_4)\, x_1^* x_3^* + (135025380000 J_3 J_9 + 55566000 J_2{}^3 J_6 - 15788682000 J_2 J_4 J_6 + 2813028750 J_2{}^2 J_8 \\
& - 2813028750 J_2 J_3 J_7 + 149333625 J_2{}^4 J_4 + 8439086250 J_3 J_4 J_5 - 151903552500 J_4 J_8 - 2509400250 J_2{}^2 J_4{}^2 \\
& + 75951776250 J_5 J_7 - 1666980000 J_3{}^2 J_6 - 4480008750 J_2 J_3{}^2 J_4 + 92610000 J_2{}^3 J_3{}^2 - 1543500 J_2{}^6 \\
& - 1389150000 J_3{}^4 - 2893401000 J_4{}^3 - 50009400000 J_6{}^2 - 67512690000 J_2 J_{10})\, x_2^{*\,2} \\
& + (1434793500 J_2{}^2 J_4 J_5 - 1629217800 J_2 J_3 J_4{}^2 + 6460738200 J_2 J_5 J_6 + 365148000 J_3{}^3 J_4 - 41806800 J_2{}^4 J_5 \\
& - 12748654800 J_3 J_4 J_6 + 1254204000 J_2 J_3{}^2 J_5 + 914457600 J_2 J_4 J_7 - 12171600 J_2{}^3 J_3 J_4 - 172254600 J_2{}^3 J_7 \\
& - 2400451200 J_2{}^2 J_9 - 714420000 J_6 J_7 - 5643918000 J_2 J_3 J_8 - 4445733600 J_4{}^2 J_5 + 14402707200 J_4 J_9 \\
& + 10811556000 J_3{}^2 J_7 - 63440496000 J_3 J_{10} - 44365482000 J_5 J_8)\, x_2^* x_3^* \\
& + (94363920 J_2{}^3 J_8 + 2592705024 J_4{}^2 J_6 - 32568480 J_3{}^2 J_4{}^2 + 57512 J_2{}^5 J_4 - 283091760 J_2{}^2 J_5{}^2 + 4386130560 J_2{}^2 J_{10} \\
& - 1905120000 J_6 J_8 - 40824000 J_7{}^2 + 34895088 J_2{}^3 J_4{}^2 + 1886976000 J_2 J_6{}^2 - 10150479360 J_5 J_9 \\
& - 109801152 J_2{}^2 J_4 J_6 + 23227223040 J_4 J_{10} + 21819168 J_2{}^4 J_6 + 3110425920 J_3 J_5 J_6 + 15630965280 J_2 J_4 J_8 \\
& + 164838240 J_2 J_3 J_4 J_5 + 635065920 J_2 J_4{}^3 - 3676609440 J_3 J_4 J_7 - 1725360 J_2{}^2 J_3{}^2 J_4 - 3397101120 J_2 J_5 J_7 \\
& - 2121396480 J_2 J_3 J_9 - 94363920 J_2{}^2 J_3 J_7 - 654575040 J_2 J_3{}^2 J_6)\, x_3^{*\,2}\,.
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{H} \;:\; 0 = {} & (20832487200\, J_7{}^3 - 98761420800\, J_6 J_7 J_8 - 14814213120\, J_6{}^2 J_9 + 140619288600\, J_5 J_8{}^2 + 21526903440\, J_5 J_7 J_9 \\
& + 192584770560\, J_4 J_8 J_9 - 29628426240\, J_3 J_9{}^2 + 6351593875200000\, J_2 J_9 J_{10} - 231472080\, J_5{}^3 J_6 \\
& + 17310682368\, J_4 J_5 J_6{}^2 - 24651776520\, J_4 J_5{}^2 J_7 + \cdots + 653457959280\, J_2{}^5 J_5 J_6 - 653460684660\, J_2{}^5 J_4 J_7 \\
& + 108909756900\, J_2{}^6 J_9 + 47040\, J_2{}^4 J_3{}^3 J_4 + 56723695560\, J_2{}^5 J_3 J_4{}^2 + 141120\, J_2{}^5 J_3{}^2 J_5 + 222264\, J_2{}^6 J_4 J_5 \\
& + 117600\, J_2{}^6 J_3 J_6 + 7056\, J_2{}^7 J_7 - 784\, J_2{}^7 J_3 J_4 - 2352\, J_2{}^8 J_5)\, x_1^{*\,4} + \cdots
\end{aligned}
$$

Questions about the reconstruction

- Q4: Where do Clebsch's formulas come from?
- Q5: What can be done for ternary quartics?
- For $g = 2$ (Bolza 1887) and $g = 3$ (Lercier,R. 2012), one can show that Mestre's strategy is available when $\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z}$.
- Q6: is it true for any genus?
- For odd genus curve with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \mathrm{Aut}(C)$, one can show that R is always zero.
- Q7: are there alternative (smart) methods when $R = 0$?
- Q8: are the different strata always rational?

How to compute isomorphisms? (Lercier-R.-Sisjling 2012)

Proposition

Let $C_i : y^2 = f_i(x)$ be hyperelliptic curves of genus g. Let c_i be covariants of f_i with non-zero discriminant and $X_i : y^2 = c_i(x)$ the associated hyperelliptic curves. Then, up to the hyperelliptic involution, $\mathit{Isom}(C_1, C_2) \subset \mathit{Isom}(X_1, X_2)$.

Hence, one can recursively reduce the computation to lower genera and/or use a new basic method to deal with this easier case.

Ultimately, we can generically use the quartic covariant $(f, f)_{n-2}$ for which we give fast formulas.

Field	Method	Genus g										
		1	2	4	8	16	32	64	128	256	512	1024
$\mathbb{F}_{10007}$	IsGL2Equivalent	0	0	0	0	0.1	0.2	0.9	6.5	39	242	1560
	IsGL2EquivFast	0	0	0	0	0	0	0.1	0.6	3.7	25	165
	IsGL2EquivCovariant	0	0	0	0	0	0	0	0	0.1	0.5	2.5
$\mathbb{Q}$	IsGL2Equivalent	0	0	0.4	15	1150	-	-	-	-	-	-
	IsGL2EquivFast	0	0	0	0	0.1	0.2	0.6	3	30	382	5850
	IsGL2EquivCovariant	0	0	0	0	0	0	0	0.2	0.6	3.4	7

Arithmetic application of covariants

Theorem

Let c be a covariant of f with non-zero discriminant and let $X : y^2 = c(x)$ be the associated curve.
Assume that X has a (hyperelliptic) model over its field of moduli and that $\# \mathrm{Aut}_K(X) = \# \mathrm{Aut}_K(C)$.
Then C has a hyperelliptic model over its field of moduli.

Rem. if X is of genus 1 then it is easy to find a model of its field of moduli and hence the procedure can be made explicit.

Example for $g = 3$ with $(\mathbb{Z}/2\mathbb{Z})^3$

$$(j_2 : j_3 : \ldots : j_{10}) = \left(0 : 0 : -\frac{25}{98} : -\frac{25}{98} : -\frac{225}{2744} : -\frac{25}{1372} : -\frac{225}{134456} : \frac{1125}{76832} : \frac{15125}{3764768}\right).$$

This gives rise to the curve $C : y^2 = f(x)$ with $\mathrm{Aut}_K(C) \simeq C_2^3$ and

$$f(x) = (-32\,\alpha^2 + 420\,\alpha - 2275)/160\,x^8 + (-12\,\alpha^2 + 140\,\alpha - 700)/25\,x^6 + \alpha\,x^4 + x^2 + (16\,\alpha^2 + 280\,\alpha - 2275)/12250$$

over $\mathbb{Q}(\alpha)$, where $\alpha^3 - 35/2\,\alpha^2 + 1925/16\,\alpha - 18375/64 = 0$.

Let $X : y^2 = c(x)$ with $\mathrm{Aut}_K(X) \simeq C_2^3$ where

$$c = (f, f)_6 = (-16\,\alpha^2 + 180\,\alpha - 875)/280\,x^4 + (24\,\alpha^2 - 630\,\alpha + 3150)/1225\,x^2 + (4\,\alpha + 35)/490.$$

$I = -75/49$, $J = -2025/343$ so $X \simeq_K \mathfrak{X} : y^2 = x^3 + 25/9\,x + 25/9$.

We compute $\phi : X \to \mathfrak{X}$ and apply it to C

$$\phi(C) : y^2 = x^8 + 160\,x^7 - 560\,x^6 - 2800\,x^5 + 64750\,x^4 - 91000\,x^3 + 3010000\,x^2 - 2225000\,x - 9696875\,.$$

More questions. . .

- Q9: Can we say something in general about the automorphism group of $(f, f)_i$ in terms of the automorphism group of f?
- Q10: How does it generalize to ternary forms?

. . . and an answer: Lüroth invariant modulo 11

$$
\begin{aligned}
&J_3^{18} + 9J_3^2J_6^8 + 4J_6^9 + 5J_3J_6^7J_9 + 7J_3^2J_6^5J_9^2 + 8J_6^6J_9^2 + 8J_3^3J_6^3J_9^3 + 9J_3^4J_6J_9^4 + 6J_6^3J_9^4\\
&+ 4J_3^3J_9^5 + 9J_3J_6J_9^5 + 9J_9^6 + 4J_3^{15}K_9 + 7J_3^3J_6^6K_9 + 5J_3J_6^7K_9 + 9J_3^2J_6^5J_9K_9\\
&+ 9J_6^6J_9K_9 + 2J_3^3J_6^3J_9^2K_9 + 6J_3J_6^4J_9^2K_9 + 2J_3^6J_9^3K_9 + 4J_3^4J_6J_9^3K_9 + 7J_3^2J_6^2J_9^3K_9\\
&+ 3J_6^3J_9^3K_9 + 5J_3^3J_9^4K_9 + 10J_3J_6J_9^4K_9 + 2J_9^5K_9 + 3J_3^2J_6^5K_9^2 + J_6^6K_9^2 + 2J_3^3J_6^3J_9K_9^2\\
&+ 3J_3J_6^4J_9K_9^2 + 5J_3^6J_9^2K_9^2 + 7J_3^4J_6J_9^2K_9^2 + 7J_3^2J_6^2J_9^2K_9^2 + 10J_3^3J_9^3K_9^2 + 5J_3J_6J_9^3K_9^2\\
&+ 7J_9^4K_9^2 + 10J_3^3J_6^3K_9^3 + 7J_3J_6^4K_9^3 + 2J_3^4J_6J_9K_9^3 + 7J_3^2J_6^2J_9K_9^3 + 4J_6^3J_9K_9^3\\
&+ 3J_3^3J_9^2K_9^3 + 10J_3J_6J_9^2K_9^3 + 2J_9^3K_9^3 + 9J_3^4J_6K_9^4 + 5J_3J_6J_9K_9^4 + 10J_9^2K_9^4 + 8J_3J_6K_9^5\\
&+ 7J_9K_9^5 + 7K_9^6 + 2J_3^{14}J_{12} + J_3^2J_6^6J_{12} + 2J_6^7J_{12} + 4J_3^3J_6^4J_9J_{12} + 7J_3J_6^5J_9J_{12}\\
&+ 5J_3^2J_6^3J_9^2J_{12} + 10J_3^5J_9^3J_{12} + 5J_3^3J_6J_9^3J_{12} + 8J_3J_6^2J_9^3J_{12} + 9J_3^2J_9^4J_{12} + 10J_6J_9^4J_{12}\\
&+ 8J_3^{11}K_9J_{12} + 2J_3^3J_6^4K_9J_{12} + 9J_3J_6^5K_9J_{12} + 9J_3^2J_6^3J_9K_9J_{12} + 3J_6^4J_9K_9J_{12}\\
&+ J_3^5J_9^2K_9J_{12} + 6J_3^3J_6J_9^2K_9J_{12} + 4J_3^2J_9^3K_9J_{12} + 5J_6J_9^3K_9J_{12} + 5J_3^2J_6^3K_9^2J_{12}\\
&+ 5J_6^4K_9^2J_{12} + 7J_3^5J_9K_9^2J_{12} + 2J_3^3J_6J_9K_9^2J_{12} + 8J_3J_6^2J_9K_9^2J_{12} + 4J_3^2J_9^2K_9^2J_{12}\\
&+ 6J_6J_9^2K_9^2J_{12} + 8J_3^5K_9^3J_{12} + 10J_3^3J_6K_9^3J_{12} + 8J_3J_6^2K_9^3J_{12} + 3J_3^2J_9K_9^3J_{12}\\
&+ 3J_6J_9K_9^3J_{12} + 8J_3^2K_9^4J_{12} + 3J_6K_9^4J_{12} + 10J_3^{10}J_{12}^2 + 2J_6^5J_{12}^2 + 3J_3^7J_9J_{12}^2\\
&+ 7J_3^3J_6^2J_9J_{12}^2 + 9J_3^4J_9^2J_{12}^2 + 8J_3^2J_6J_9^2J_{12}^2 + 10J_6^2J_9^2J_{12}^2 + 8J_3J_9^3J_{12}^2 + 7J_3^7K_9J_{12}^2\\
&+ 9J_3J_6^3K_9J_{12}^2 + 2J_3^4J_9K_9J_{12}^2 + J_3^2J_6J_9K_9J_{12}^2 + 7J_6^2J_9K_9J_{12}^2 + 4J_3J_9^2K_9J_{12}^2\\
&+ 10J_3^4K_9^2J_{12}^2 + 8J_3^2J_6K_9^2J_{12}^2 + 9J_6^2K_9^2J_{12}^2 + J_3J_9K_9^2J_{12}^2 + 4J_3K_9^3J_{12}^2 + 5J_3^6J_{12}^3\\
&+ 7J_3^4J_6J_{12}^3 + 4J_3^2J_6^2J_{12}^3 + 5J_6^3J_{12}^3 + 9J_3^3J_9J_{12}^3 + 8J_3J_6J_9J_{12}^3 + 9J_9^2J_{12}^3 + 2J_3^3K_9J_{12}^3\\
&+ 4J_3J_6K_9J_{12}^3 + 5K_9^2J_{12}^3 + 7J_3^2J_{12}^4 + 2J_6J_{12}^4 + 6J_3^{14}K_{12} + 2J_3^2J_6^6K_{12} + 3J_6^7K_{12}\\
&+ 5J_3^3J_6^4J_9K_{12} + 7J_3J_6^5J_9K_{12} + 3J_3^2J_6^3J_9^2K_{12} + J_6^4J_9^2K_{12} + \ldots \text{ (1164 monomials)}
\end{aligned}
$$