1. Introduction

Motivation: We want to study curve covers \( f : C \to \mathbb{P}^1 \) over a field \( K \) satisfying the following conditions:

(i) \( C \) is a smooth hyperelliptic curve of genus \( g_C = 3 \);
(ii) \( f \) has degree \( \deg(f) = 4 \);
(iii) \( f \) has ramification type \( (2, 2)^4(2, 1, 1)^4 \);
(iv) \( f \) has monodromy group \( G_f \cong S_4 \).

Tasks: 1) Find explicit equations for such curve covers.
2) Describe the Hurwitz space of such covers, i.e., determine the space which classifies equivalence classes of such covers.

Remark: 1) Covers of the above type are of interest in cryptography in connection with Ben Smith’s attack on the security of hyperelliptic genus 3 curves over \( \mathbb{F}_q \) (cf. G. Frey’s lecture).
2) If we drop the condition “hyperelliptic” in the above hypotheses, then the answer to Task 2 can be obtained from the usual techniques of the theory of Hurwitz spaces (cf. Fried/Völklein).

However, these techniques do not easily extend to include the above situation.
2. An example

Consider the polynomial

\[
F(T, X) = 12TX^4 + 12T(2T - 1)X^3 + (28T^2 + 27T - 88)X^2 + 18T(2T - 3)X - 3T(8T - 17).
\]

**Facts:** (i) The equation \( F(T, X) = 0 \) defines a smooth curve \( C/\mathbb{Q} \) of genus 3 which has good reduction \( C_p \) at all primes \( p > 5 \) except for \( p \in S_1 := \{11, 13, 17, 19, 47, 191\} \).

(ii) The projection \((T, X) \mapsto T\) defines a cover \( f : C \to \mathbb{P}^1_{\mathbb{Q}} \) of degree 4, as well as degree 4 covers \( f_p : C_p \to \mathbb{P}^1_{\mathbb{F}_p} \) (for \( p > 5 \)).

(iii) \( f \) has ramification type \((2, 2)\) at \( T = 0, 1, -1, 2 \) and simple ramification type \((2, 1, 1)\) at 4 other points (over \( \overline{\mathbb{Q}} \)). Moreover, the same is true for \( f_p \) if \( p > 5 \) except for \( p \in S_2 = S_1 \cup \{7, 31, 379\} \).

(iv) The Galois group of \( F \) over \( \mathbb{Q}(T) \) is \( \text{Gal}(F) \simeq S_4 \), i.e., the monodromy group of \( f \) is \( G_f \simeq S_4 \). Moreover, the same is true for \( f_p \) if \( p > 19 \), except when \( p \in S_2 \).

**Remark:** By considering other examples, one can show that curve covers satisfying conditions (i)–(iv) exist over \( K \) whenever \( \text{char}(K) > 7 \).
3. Hyperelliptic Hurwitz spaces (General Theory)

**Fix:** an integer \( n \geq 3 \) and a field \( K \), and consider \( K \)-covers

\[ f : C \rightarrow \mathbb{P}_K^1 \]

satisfying the following conditions:
(i) \( C/K \) is a smooth hyperelliptic curve of genus \( g_C = n - 1 \);
(ii) \( \deg(f) = n \), and \( f \circ \omega_C \neq f \), where \( \omega_C \) is the hyperelliptic involution of \( C \).

**Definition:** The set \( \mathcal{H}_n(K) \) of isomorphism classes of such covers is called the *Hurwitz space of hyperelliptic covers of degree \( n \) (and of genus \( n - 1 \)).

**Rigidification:** Consider the set \( \mathcal{H}_n^{\text{rig}}(K) \) of isomorphism classes of triples \((C, f, \pi)\) with \((C, f) \in \mathcal{H}_n(K)\) and a fixed hyperelliptic cover

\[ \pi : C \rightarrow \mathbb{P}_K^1. \]

**Note:** Since \( \pi \) is unique up to an automorphism of \( \text{Aut}(\mathbb{P}_K^1) \),

\[ \mathcal{H}_n(K) = \text{Aut}(\mathbb{P}_K^1) \backslash \mathcal{H}_n^{\text{rig}}(K). \]

**Observation:** Given \((C, f, \pi) \in \mathcal{H}_n^{\text{rig}}(K)\), \( \exists! \) morphism

\[ j_C : C \rightarrow \mathbb{P}_K^1 \times \mathbb{P}_K^1 \]

such that \( f = \text{pr}_1 \circ j_C, \pi = \text{pr}_2 \circ j_C \), where \( \text{pr}_i : \mathbb{P}_K^1 \times \mathbb{P}_K^1 \rightarrow \mathbb{P}_K^1 \) is the \( i^{th} \) projection map. Also:

- \( j_C \) is a closed immersion (so \( C \simeq j_C(C') \));
- \( D_C := j_C(C) \) is a divisor on the surface \( \mathbb{P}_K^1 \times \mathbb{P}_K^1 \) and

\[ D_C \sim D_{2,n} := 2(P \times \mathbb{P}_K^1) + n(\mathbb{P}_K^1 \times P), \text{ for } P \in \mathbb{P}(K). \]
**Proposition 1:** The rule \((C, f, \pi) \mapsto D_C\) induces a bijection

\[ \kappa_n : H_{\text{rig}}^n(K) \xrightarrow{\sim} |D_{2,n}|_{\text{sm}}^K, \]

where \(|D_{2,n}|_{\text{sm}}^K \subset |D_{2,n}|_K\) denotes the subset of smooth divisors in the linear system \(|D_{2,n}|_K\).

**Remarks:**

1) Since \(|D_{2,n}|_K \simeq \mathbb{P}^{3n+2}\), this means that we can identify \(H_{\text{rig}}^n(K)\) with a non-empty, open subset of \(\mathbb{P}^{3n+2}\).

2) If we fix homogeneous coordinates on \(\mathbb{P}^1\), then each divisor \(D \in |D_{2,n}|\) is given by an equation \(F(T_0, T_1; X_0, X_1) = 0\), where \(F\) is homogeneous of degree 2 in \(T_0, T_1\) and of degree \(n\) in \(X_0, X_1\), i.e.,

\[
F(T_0, T_1; X_0, X_1) = \sum_{i=0}^{n} \sum_{j=0}^{2} r_{ij} X_0^i X_1^{n-i} T_0^{2-j} T_1^j,
\]

where \(r_{ij} \in K\). For simplicity, we write this polynomial in its affine (de-homogenized) form

\[
F(T, X) = \sum_{i=0}^{n} \sum_{j=0}^{2} r_{ij} X^{n-i} T^j.
\]

**Proposition 2:** Let \(C \in |D_{2,n}|\) be given by \(F(T_0, T_1, X_0, X_1)\). If \(\text{char}(K) \neq 2\), then \(C \in |D_{2,n}|_{\text{sm}}\) if and only if its discriminant

\[
D^h_F(X_0, X_1) = A_1^2 - 4A_0A_2, \quad \text{where} \quad A_j = \sum_{i=0}^{n} r_{ij} X_0^i X_1^{n-i},
\]

is separable, i.e., \(D^h_F\) factors over \(\overline{K}\) into \(2n\) distinct linear factors.

**Assume henceforth:** char$(K) \neq 2$.

**Notation:** Fix coordinates on $\mathbb{P}^1_K$. Let $P_\infty = (0 : 1)$, and write $P_a = (1 : a)$ for $a \in K$. Moreover, put $P_{a,b} = (P_a, P_b) \in (\mathbb{P}^1 \times \mathbb{P}^1)(K)$, for $a, b \in K_\infty = K \cup \{\infty\}$.

Furthermore, let $\mathcal{H}^{\text{rig}}_{4,3}$ denote the subset of curves $C \in |D_{2,4}|^{\text{sm}}$ satisfying the following conditions:

1. $f^*_C(P_0) = 2P_{0,\infty} + 2P_{0,0}$,
2. $f^*_C(P_1) = 2P_{1,1} + 2P_{1,\alpha}$, for some $\alpha \in K, \alpha \neq 1$
3. $f^*_C(P_{-1}) = 2D$, for some $D \in \text{Div}(C)$, $D \neq P_{-1,\infty} + P_{-1,0}, D \neq 2P, \forall P$.

Here $f_C = (pr_1)|_C : C \to \mathbb{P}^1_K$ is the induced degree 4 cover.

**Thus:** Each $C \in \mathcal{H}^{\text{rig}}_{4,3}$ is smooth of genus 3, and the cover $f_C$ is ramified of type $(2, 2)$ at the points $P_0, P_1, P_{-1} \in \mathbb{P}^1_K(K)$.

**Moreover:** For $t \in K \setminus \{0, 1, -1\}$, let $\mathcal{H}^{\text{rig}}_{4,4,t}$ denote the subset of those $C \in \mathcal{H}^{\text{rig}}_{4,3}$ which are also ramified of type $(2, 2)$ at $P_t$:

4. $f^*_C(P_t) = 2D_t$, with $D_t \neq 2P$, for any $P \in C(\overline{K})$.

**Theorem 1:** The Hurwitz space $\mathcal{H}^{\text{rig}}_{4,3}$ is a smooth, rational variety of dimension. More precisely, $\mathcal{H}^{\text{rig}}_{4,3}$ is covered by two open subsets which are isomorphic to open subsets of $\mathbb{A}^5$.

**Remark:** The curves $C \in \mathcal{H}^{\text{rig}}_{4,3}$ can be described explicitly in terms of their associated equations $F(T, X) = 0$. 
**Notation:** Let

\[ \mathcal{H}_{4,4,t}^* = \{ C \in \mathcal{H}_{4,3,t}^{\text{rig}} : P_{-1,\infty} \notin C, P_{t,\infty} \notin C \} \].

**Theorem 2:** The Hurwitz space \( \mathcal{H}_{4,4,t}^* \) consists of two disjoint rational components:

\[ \mathcal{H}_{4,3,t}^* = \mathcal{H}_{4,3,t,1}^* \cup \mathcal{H}_{4,3,t,2}^* \]

Moreover, all the covers in \( \mathcal{H}_{4,3,t,1}^* \) factor over a quadratic cover, whereas in general the covers in \( \mathcal{H}_{4,3,t,2}^* \) do not admit such a factorization.

**Remarks:**

1) A similar result should also be true for \( \mathcal{H}_{4,3,t}^{\text{rig}} \) (in place of \( \mathcal{H}_{4,3,t}^* \)), but this has not been proved yet.

2) Due to the presence of certain exceptional (lower-dimensional) subvarieties, the proof of Theorem 2 is rather complicated.
5. Explicit equations.

Notation: For $r_{01}, r_{11}, r_{12}, t \in K$, put

\[
\begin{align*}
    a_0 &= 1 - 2r_{01} \\
    a_1 &= r_{12} - r_{11} \\
    a_2 &= r_{12} + r_{11} \\
    a_3 &= r_{01}r_{11} + r_{01}r_{12} - r_{11} \\
    a_5 &= (1 - r_{01})t + r_{01} \\
    a_6 &= r_{12}t + r_{11} \\
    \alpha &= -\frac{1}{2}(r_{11} + r_{12} + 2)
\end{align*}
\]

For $a_0a_5 \neq 0$, let

\[
F_1(T, X) = AX^4 + BX^3 + CX^2 + \alpha BX + \alpha^2 A,
\]

in which

\[
\begin{align*}
    A &= A(T) = r_{01}T + (1 - r_{01})T^2, \\
    B &= B(T) = r_{11}T + r_{12}T^2, \\
    C &= C(T) = r_{20} + r_{21}T + (\alpha^2 + 4\alpha + 1 - r_{20} - r_{21})T^2,
\end{align*}
\]

with

\[
\begin{align*}
    r_{20} &= \frac{ta_3^2}{4a_0a_5} \quad \text{and} \quad r_{21} = \frac{4a_0(4\alpha r_{01} + (\alpha + 1)^2) - a_1^2}{8a_0}.
\end{align*}
\]

Moreover, if also $dq \neq 0$, where $d = 4\alpha a_0a_3$ and

\[
q = a_2(2r_{01}a_2 + a_1(2t - 3a_5) - 2a_5r_{11}) + 2(t - 1)r_{11}^2,
\]

then put

\[
F_2(T, X) = F_1(T, X) + \frac{d}{q}G(T, X), \quad \text{where}
\]

\[
G(T, X) = (c_2(1 - T^2) + a_6T(1 - T))X^2 + c_3T(1 - T)X + c_4T(1 - T),
\]

with

\[
\begin{align*}
    c_2 &= \frac{ta_3}{a_0}, \quad c_3 = \frac{a_1a_6}{2a_0}, \quad c_4 = -\frac{\alpha a_1a_2a_5a_6}{q}.
\end{align*}
\]
Theorem 3: Let \( t \in K^\bullet := K \setminus \{0, 1, -1\} \). If \( C \in \mathcal{H}_{4,3,t,1}^* \), then \( \exists! r_{01}, r_{11}, r_{12} \in K \) such that the associated equation \( F_1(T, X) = 0 \) gives \( C \). Moreover, the discriminant

\[
D_{F_1}(X) := A_1^2 - 4A_0A_2, \quad \text{where} \quad A_j = \sum_{i=0}^{4} r_{ij}X^{4-i}
\]
is separable of degree 8 and the following inequalities hold:

\( (5) \quad \alpha \neq 1, \quad a_1^2 \neq 16^2a_0^2\alpha \quad \text{and} \quad a_6^2 \neq 16a_5^2\alpha. \)

Conversely, if \( F_1(T, X) \) is as above (including (5) and the discriminant condition), then the equation \( F_1(T, X) = 0 \) defines a curve \( C \in \mathcal{H}_{4,3,t,1}^* \).

Theorem 4: (a) Let \( t \in K^\bullet \) and let \( r_{01}, r_{11}, r_{12} \in K \) satisfy \( a_0a_5dq \neq 0 \) and the inequalities

\( (6) \quad \alpha \neq 1, \quad a_1^2 \neq 16^2a_0^2(\alpha - \beta), \quad a_6^2 \neq 16a_5^2(\alpha - (t - 1)\beta), \)

where \( \beta = \frac{d_6}{a_0^q}. \) Then the associated equation \( F_2(T, X) = 0 \) defines a curve \( C \in \mathcal{H}_{4,3,t,2}^* \), provided that its discriminant \( D_{F_2}(X) \) is separable of degree 8.

(b) The set of curves \( C \) obtained by the equations of part (a) form an open subset \( \mathcal{H}'_{4,3,t,2} \) of \( \mathcal{H}_{4,3,t,2}^* \). The complement

\[
\mathcal{H}''_{4,3,t,2} = \mathcal{H}_{4,3,t,2}^* \setminus \mathcal{H}'_{4,3,t,2}
\]

consists of two disjoint rational varieties of dimension 2.

Remark: In our paper we give the explicit equations for the two families which describe the two components of \( \mathcal{H}''_{4,3,t,2} \).
Remark: The proofs of the above theorems are very computational and use MAPLE to simplify complicated algebraic expressions. They also use the following technical fact which allows us to analyze the $(2, 2)$-ramification condition.

Lemma: Let $Q(X) = AX^4 + BX^3 + CX^2 + DX + E \in K[X]$, where $A \neq 0$. The following are equivalent:

(i) $Q(X) = Aq(X)^2$, for some $q(X) = X^2 + bX + c$;
(ii) $8A^2D = B\Delta$ and $64EA^3 = \Delta^2$, where $\Delta = 4AC - B^2$.

Moreover, if this holds, then

$$b = B/(2A) \quad \text{and} \quad c = \Delta/(8A^2),$$

and so $q(X)$ has distinct roots in $\overline{K}$ if and only if

$$B^2 - 2A\Delta = 3B^2 - 8AC \neq 0.$$
6. Ramification types.

**Definition:** A curve cover $f : C \rightarrow C_0$ has ramification type $(e_1, \ldots, e_r)$ at $P_0 \in C_0(K)$ if $e_1 \geq \ldots, e_r \geq 1$ with $e_1 > 1$ and if there exist distinct points $P_1, \ldots, P_r \in C(\overline{K})$ such that

$$f^*(P_0) = \sum_{i=1}^r e_i P_i.$$ 

The list of ramification types of all points is called the ramification type of the cover.

**Example:** If $C \in \mathcal{H}_{4,3,t}^{\text{rig}}$, then the associated cover $f_C : C \rightarrow \mathbb{P}^1$ has ramification type $(2, 2)$ at the points $P_0, P_1, P_{-1}$ and $P_t \in \mathbb{P}^1(K)$.

**Notation:** If $F(T, X) \in K[T, X]$ is a polynomial, then let

$$D_{F,X}(T) = \text{disc}_X(D(F)) \in K[T]$$

denote the discriminant of $F$ (viewed as a polynomial in $X$).

**Proposition 3:** If $F(T, X) = 0$ describes a curve $C$ in $\mathcal{H}_{4,3,t}^{\text{rig}}$, then $\deg_T(D_{F,X}) = 12$ and

$$D_{F,X}^*(T) := D_{F,X}(T)/(T(T^2 - 1)(T - t))^2 \in K[T].$$

Moreover, $f_C$ has ramification type $(2, 2)^4(2, 1, 1)^4$ if and only if $D_{F,X}^*(T)$ is a separable polynomial, which is equivalent to

(7) \quad \text{disc}_T(D_{F,X}^*) \neq 0.

Thus, the set of $C \in \mathcal{H}_{4,3,t}^{\text{rig}}$ with $f_C$ of ramification type $(2, 2)^4(2, 1, 1)^4$ is an open subset of $\mathcal{H}_{4,3,t}^{\text{rig}}$. 
7. Monodromy groups.

Recall: By field theory, each separable cover $f : C \to C_0$ has a Galois hull

$$\tilde{f} : \tilde{C} \to C_0.$$ 

This a Galois cover which factors over $f$, i.e., $\tilde{f} = f \circ f'$, for some $f' : \tilde{C} \to C$, and which is minimal with these properties. The Galois group

$$G_f = \text{Gal}(f)$$

is called the monodromy group of the cover $f$.

Proposition 4: Let $F(T, X) = 0$ define a curve $C \in \mathcal{H}_{4,3,t}^{\text{rig}}$, and let $G_F = G_{f_C}$ be the monodromy group of the associated cover. Then the following are equivalent:

(i) $G_F \simeq D_4$ or $G_F \simeq S_4$;

(ii) $D_{F,X}^*(T)$ is not a square (in $\overline{K}(T)$).

On the other hand, if $D_{F,X}^*(T)$ is a square, then either $G_F \simeq A_4$ or $G_F \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In particular, $G_F$ can never be a cyclic group.

Remark: A useful method for distinguishing between the $D_4$ and the $S_4$ case is to study the Lagrange resolvent (or cubic resolvent) of $F$. 
8. The Lagrange Resolvent

**Definition:** The *Lagrange resolvent* of a general quartic

\[ f(x) = ax^4 + bx^3 + cx^2 + dx + e \]

is the monic cubic polynomial \( r_f(x) \) which is defined by

\[ r_f(x) = x^3 - cx^2 + (bd - 4ae)x + a(4ce - d^2) - b^2e. \]

**Remarks:**
1) If \( f \) is monic, then this definition of \( r_f \) agrees with the usual definition. In general case we have (when \( a \neq 0 \)) the relation

\[ r_f(ax) = a^3 r_{\tilde{f}}(x), \]

where \( \tilde{f}(x) = f(x)/a \) is the associated monic polynomial.

2) It is a remarkable and useful fact that

\[ \text{disc}(r_f) = \text{disc}(f). \]

**Proposition 5:** Let \( F(T, X) = 0 \) define a curve \( C \in \mathcal{H}_{4,3,t}^{\text{rig}} \), and suppose that \( D_{F,X}^*(T) \) is not a square. Then

\[ G_F \cong S_4 \iff r_F(X) \text{ is irreducible over } K(T). \]

**Lemma:** If \( f(X) \in k[X] \) is an irreducible quartic of the form

\[ f(X) = aX^4 + bX^3 + cX^2 + abX + a^2a, \]

then \( \text{Gal}_f \cong D_4 \) or \( \text{Gal}_f \cong \mathbb{Z}/4\mathbb{Z} \) or \( \text{Gal}_f \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \).

**Proof.** \( r_f(2a\alpha) = 0 \), so \( r_f \) is reducible. Thus, the assertion follows from Proposition 4.11 of Hungerford’s *Algebra*, p. 273.
Corollary: Let $C \in \mathcal{H}_{3,4,t,1}^*$ with associated polynomial $F_1(T, X)$. Then
\[ G_{F_1} \simeq D_4 \iff D_{F,X}^* \text{ is not a square}. \]
On the other hand, if $D_{F,X}^*$ is a square, then $G_{F_1} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Theorem 5: Let $C \in \mathcal{H}_{3,4,t,2}'$ be defined by a polynomial equation $F_2(X, T) = 0$, with $F_2$ as in Theorem 4. Suppose that $D_{F_2,X}^*$ is separable, i.e., the discriminant condition (7) holds. Then
\[ G_{F_2} \simeq S_4 \iff \alpha a_1 \neq 0. \]

Corollary: If $\text{char}(K) = 0$ or $\text{char}(K) > 7$, then there is a non-empty open subset $U_{3,4,t}$ of $\mathcal{H}_{3,4,t,2}'$ such that each $C \in U$ with its associated cover $f_C : C \rightarrow \mathbb{P}^1$ satisfies the conditions (i) – (iv) of the introduction.

Remark: However, $U_{3,4,t}$ is not the full (rigid) Hurwitz space of such covers because one of the two components of the complement $\mathcal{H}_{3,4,t,2}''$ also produces examples of curve covers satisfying (i) – (iv).
9. The associated (2,3)-cover.

Proposition 5: Let \( f : C \rightarrow \mathbb{P}_K^1 \) be a curve cover satisfying conditions (i) – (iv), and let \( F(T, X) = 0 \) be its defining equation. Let \( r_F(T, X) \) be the Lagrange resolvent of \( F \) over \( K(T) \).

(a) The curve \( C_{r_F} : r_F(T, X) = 0 \) is rational. If we fix a parametrization \( (T(U), X(U)) \) of \( C_{r_F} \), then the rational function \( T(U) \in K(U) \) defines a cubic cover

\[
f_3 : \mathbb{P}^1 \rightarrow \mathbb{P}^1.
\]

(b) Let \( C' \) be the (hyperelliptic) curve defined by the equation

\[
Y^2 = X(U)^2 - 4A(T(U))E(T(U)),
\]

where \( A(T) \) and \( E(T) \) are the highest and constant coefficients of \( F(T, X) \). If \( f_2 : C' \rightarrow \mathbb{P}^1 \) denotes the associated hyperelliptic cover, then \( C' \) has genus 3, and the Galois hull \( \tilde{f} : \tilde{C} \rightarrow \mathbb{P}^1 \) factors over \( f_3 \circ f_2 \). Moreover, \( \tilde{f} \) is also the Galois hull of \( f_3 \circ f_2 \).

Remarks: 1) MAPLE has a nice program which computes a parametrization of any rational plane curve \( g(x, y) = 0 \).

2) We thus have:

\[
\begin{array}{c}
\tilde{C} \\
\downarrow \\
C'' \\
\downarrow \\
C'''
\end{array}
\]

\[
\begin{array}{c}
\downarrow \\
f_3 \\
\downarrow \\
\mathbb{P}^1
\end{array}
\]

\[
\begin{array}{c}
C \\
\downarrow \\
f_2 \\
\downarrow \\
\mathbb{P}^1
\end{array}
\]

\[
\begin{array}{c}
\downarrow \\
f_3 \\
\downarrow \\
\mathbb{P}^1
\end{array}
\]

\[
\begin{array}{c}
\downarrow \\
f_2 \\
\downarrow \\
\mathbb{P}^1
\end{array}
\]
10. Connection with the attack of Ben Smith.

**Given:** A hyperelliptic cover $f_2 : C' \rightarrow \mathbb{P}^1_{\mathbb{F}_q}$.

**Construct:** a curve $C/\mathbb{F}_q$ of genus 3 and a $(3, 2)$-correspondence $C''$ between $C$ and $C'$

\[ C'' \]
\[ \xrightarrow{3} \quad \xrightarrow{2} \]
\[ C \quad \xrightarrow{} \quad C' \]

such that the induced homomorphism on the Jacobians is an isogeny:

\[ T_{C''} : J_{C''} \rightarrow J_C. \]

**Note:** If $C$ is NOT hyperelliptic, then the attack is successful (the cryptosystem based on $C''$ is not secure).

**Method (Donagi/Livné/Smith):** Use the trigonal construction: construct a cubic (sub)cover $f_3 : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ such that $f_3 \circ f_2$ has a “special” ramification structure. Smith gives a geometric construction for obtaining $C$ from $f_3$ and $f_2$.

**Main idea (via Galois theory):** The hypotheses imply that $f_6 := f_3 \circ f_2$ has monodromy group $S_4$. If $\tilde{f}_6 : \tilde{C} \rightarrow \mathbb{P}^1$ is the Galois hull, then $C := \tilde{C}/S_3$ is the associated genus 3 curve.

**Thus:** The construction of §9 is inverse to that of Ben Smith.