CONSTRUCTING CURVES OF LARGE RANK USING COMPOSITE POLYNOMIALS

ARVIND SURESH

ABSTRACT. Let $k$ be a number field. We refine a construction of Mestre–Shioda to construct (infinite) families of hyperelliptic curves $X/k$ having a record number of rational points and record Mordell–Weil rank relative to the genus of $g$ of $X$. Over $k = \mathbb{Q}$, we obtain modest improvements on the current published records, and these improvements become more significant as $k$ gets larger. For example, we obtain curves over the real cyclotomic field $k := \mathbb{Q}(\cos(\pi/(g + 1)))$ having at least $16(g + 1)$ $k$-points and rank at least $8g$. The defining equations for the curves are closely related to the classical Chebyshev polynomials, and in special cases, we recover families studied (for example) by Mestre, Shioda, Brumer, and Tautz–Top–Verberkmoes.

CONTENTS

1. Introduction 1
2. Tools for bounding ranks of hyperelliptic curves 7
3. The specialization method 10
4. The Mestre–Shioda construction 11
5. Strategy behind improvement 13
6. Constructing the splitting field $K_f$ of $\mathbb{f}(x)$ over $\mathbb{K}$ 14
7. Polynomials having cyclic and dihedral monodromy groups 16
8. The rational function fields $\mathbb{K}_{\text{cyc}}^n$, $\mathbb{K}_{\text{dih}}^n$, and $\mathbb{K}_{\text{re}}^n$. 20
9. Defining the curves and stating the point and rank bounds 22
10. First reduction: partner curves 27
11. $\hat{Z}$-systems and new parts decompositions 29
12. Second reduction: From $[W_n^\ast]$ to $[V_n^\ast]$ 33
13. Determining $\rho_n^\text{cyc}$, $\rho_n^\text{re}$, and $\rho_n^\text{im}$, and finishing the proof of Theorem 9.17 34
14. Non-isotriviality of the Real, Imaginary, and Dihedral families 37
15. Complex multiplication of $A_n^\text{cyc} / \bar{K}$ and the proof of Theorem 1.13 39
References 41

1. INTRODUCTION

Let $k$ be a number field, let $X/k$ be a nice (i.e. smooth, projective, geometrically integral) curve of genus $g$, and let $J_X/k$ denote the Jacobian of $X$. The Mordell–Weil Theorem says that $J_X(k)$ is a finitely generated abelian group. The rank of $X/k$ is the integer

$$\text{rk } X/k := \dim_{\mathbb{Q}}(J_X(k) \otimes_{\mathbb{Z}} \mathbb{Q}).$$

Faltings’ Theorem [Fal83, Satz 7], formerly known as the Mordell Conjecture, says that if $g \geq 2$, then the set $X(k)$ of $k$-rational points of $X$ is finite. Given these finiteness theorems, it is natural to
wonder, for a fixed genus $g$ and number field $k$, how large the integers $#X(k)$ and $\text{rk } X/k$ can be. We define two constants, taking values in $\mathbb{N} \cup \{\infty\}$, as follows:

\[
R(k, g) := \sup\{R \mid \text{rk } X/k \geq R \text{ for infinitely many genus } g \text{ curves } X/k\}, \\
N(k, g) := \sup\{N \mid #X(k) \geq N \text{ for infinitely many genus } g \text{ curves } X/k\}.
\] (1.1)

Above, and for the rest of the article, by “infinitely many curves over $k$,” we mean “infinitely many nice curves that are pairwise non-isomorphic over an algebraic closure $\bar{k}$.”

For any number field $k$ and positive $g$, whether $R(k, g) < \infty$ is an open question. On the other hand, it is a theorem of Caporaso, Harris, and Mazur [CHM97, Theorem 1.2] that if the Weak Lang Conjecture [CHM97, Conjecture A] is true (which is not currently known) then $N(k, g) < \infty$ for any number field $k$ and $g \geq 2$ (i.e. $#X(k) \leq N(k, g)$ for all but finitely many ($\bar{k}$-isomorphism classes of) genus $g$ curves $X/k$).

A genus 1 curve $X/k$ with a rational point is an elliptic curve, and $X \cong J_X$. The question of whether $R(\mathbb{Q}, 1) < \infty$ has been the subject of multiple folklore conjectures; the papers [PPVW19, Wat15] give heuristics that suggest $R(\mathbb{Q}, 1) \leq 21$ (in other words, they predict that only finitely many elliptic curves over $\mathbb{Q}$ have rank exceeding 21). For $g \geq 2$, to the best of our knowledge, there exist no such heuristics, nor a folklore conjecture in either direction.

Producing an infinite set of genus $g$ curves $X/k$ satisfying $\text{rk } X/k \geq R$ and $#X(k) \geq N$ would yield lower bounds $R(k, g) \geq R$ and $N(k, g) \geq N$. The standard way to do this is by the method of specialization; one constructs over the function field $k(V)$ of a $k$-variety $V$ a curve $X/k(V)$ that has the desired properties (genus $g$, many rational points, large rank), and then one takes specializations of $X$ that preserve these properties. The use of the specialization method to construct curves of high rank originated in the work of Néron [Nér52, Nér56], who proved a theorem [Nér52, Théorème 6] on the injectivity of the specialization map (cf. 3.2) for Jacobians of curves $X/k(V)$, with $V$ rational over $k$, and applied it to construct infinitely many elliptic curves of rank at least 10 (i.e. $R(\mathbb{Q}, 1) \geq 10$), and for $g \geq 2$, infinitely many genus $g$ curves of rank at least $3g + 6$ (see also [SU99] for a correction of Néron’s original claim of $3g + 7$).

Mestre [Mes91a, Mes91b] constructed a genus $g$ curve $\mathbb{X}/\mathbb{K}$, with $\mathbb{K}$ a rational function field over $\mathbb{Q}$, having at least $8g + 12$ rational points. His construction yields $N(\mathbb{Q}, g) \geq 8g + 12$, and he used it in the case $g = 1$ to prove $R(\mathbb{Q}, 1) \geq 12$. Shioda [Shi98] refined and generalized Mestre’s construction and proved $R(\mathbb{Q}, g) \geq 4g + 7$ and $N(\mathbb{Q}, g) \geq 8g + 16$ for all $g \geq 2$; we refer to this as the Mestre–Shioda construction (see Section 4).

In this article, we present a refinement of the Mestre–Shioda construction which allows us to improve on the known lower bounds for the constants $N(k, g)$ and $R(k, g)$, for various pairs $(k, g)$. In fact, our main result, Theorem 1.3 below, gives bounds for the following natural generalization of the constant $R(k, g)$- for a finite abelian group $B$, we define the constant

\[
R(k, g; B) := \sup\{R \mid J_X(K) \supset Z^R \oplus B \text{ for infinitely many genus } g \text{ curves } X/k\}. 
\] (1.2)

Note that $R(K, g; 0) = R(k, g)$. Below, and in the rest of the article, $Z_n$ denotes the cyclic group of order $n$, $V_4$ denotes the Klein-4 group $Z_2 \times Z_2$, $\xi_n$ as usual denotes the primitive $n$-th root of unity $e^{2\pi i/n}$, and $\lambda_n$ denotes the real number $\xi_n + \xi_n^{-1} = 2 \cos(2\pi/n)$ (so that $\mathbb{Q}(\lambda_n)$ is the maximal real subfield of the $n$-th cyclotomic field $\mathbb{Q}(\xi_n)$).
Theorem 1.3 (Proved in 9.20). Let \( n, d, \) and \( g \) be positive integers such that \( nd \) equals one of the values in the first column of Table 1.4 below, and let \( k \) be a number field that contains the number \( \alpha \) in the second column. Then, we have the bounds

\[
N(k, g) \geq N \quad \text{and} \quad R(k, g; B) \geq R,
\]

where \( B \) denotes the group in the third column and \( N \) (resp. \( R \)) denotes the integer in the fourth column (resp. last three columns, depending on the condition satisfied by \( d \) in the last row).

| \( nd \) | \( \alpha \) | \( B \) | \( N \) | \( R \) |
|---|---|---|---|---|
| \( 2g + 2 \) | \( \lambda_n \) | 0 | \( 8g + 4n + 8 \) | \( 8g \) | \( 4g + 2n + 3 \) |
| \( 2g + 1 \) | \( \lambda_n \) | 0 | \( 8g + 4n + 5 \) | \( 8g \) | \( 4g + 2n + 2 \) |
| \( 2g \) | \( \lambda_{2n} \) | \( \mathbb{Z}_2 \) | \( 8g + 4n + 2 \) | \( 8g \) | \( 4g + 2n \) |
| \( 2g - 1 \) | \( \zeta_n \) | \( V_4 \) | \( 8g + 4n - 1 \) | \( 8g - 4 \) | \( 4g + 2n - 2 \) |
| \( g + 1 \) | \( \zeta_n \) | 0 | \( 8g + 8n + 8 \) | \( 8g - 4 \) | \( 4g + 4n + 3 \) |

\[ d = 1 \quad d = 2 \quad d \geq 3 \]

Table 1.4: Bounds for \( k \) containing \( \lambda_n, \lambda_{2n}, \) or \( \zeta_n \)

1.5. The case \( k = \mathbb{Q} \). For a given number field \( k \), there are finitely many integers \( n \) for which \( k \) contains \( \lambda_n, \zeta_n, \) or \( \lambda_{2n} \). For each such \( n \), by allowing \( d \) (and therefore also \( g \)) to vary in Theorem 1.3, we obtain bounds for all sufficiently large genera \( g \) comprising certain congruence classes.

For example, \( \mathbb{Q} \) contains \( \lambda_n \) for \( n = 2 \), so putting \( 2d = 2g + 2 \) in the first row of Table 1.4 we recover Shioda’s bounds \( N(\mathbb{Q}, g) \geq 8g + 16 \) and \( R(\mathbb{Q}, g) \geq 4g + 7 \) (for \( g \geq 2 \)) from [Shi98]. This is not a coincidence; our method is a generalization of [Shi98] (see Example 5.7).

Observe now that \( \mathbb{Q} \) also contains \( \lambda_n \) if \( n = 3, 4, \) or \( 6 \). By setting

\[
6d = 2g + 2, \quad 4d = 2g + 2, \quad 3d = 2g + 1, \quad 3d = 2g, \quad \text{and} \quad d = 2g - 1
\]

in Table 1.4, respectively, we obtain the following bounds that improve on [Shi98].

Corollary 1.6. For any positive integer \( g \), we have the following bounds.

| Condition on \( g \) | \( B \) | \( N(\mathbb{Q}, g) \) | \( R(\mathbb{Q}, g; B) \) |
|---|---|---|---|
| \( g \equiv 2 \) (mod 3) | 0 | \( 8g + 32 \) | \( 4g + 15 \) if \( g \geq 8 \) |
| \( g \equiv 1 \) (mod 2) | 0 | \( 8g + 24 \) | \( 4g + 11 \) if \( g \geq 5 \) |
| \( g \equiv 1 \) (mod 3) | 0 | \( 8g + 17 \) | \( 4g + 8 \) if \( g \geq 4 \) |
| \( g \equiv 0 \) (mod 3) | \( \mathbb{Z}_2 \) | \( 8g + 14 \) | \( 4g + 6 \) if \( g \geq 6 \) |
| \( g \equiv 1 \) (mod 2) | \( V_4 \) | \( 8g + 3 \) | \( 4g \) if \( g \geq 1 \) |

Table 1.7: Bounds for \( k = \mathbb{Q} \)

1.8. New records for \( \mathbb{Q} \). We now summarize the state of the art for \( k = \mathbb{Q} \) and see where we obtain new records.
We have \( N(\mathbb{Q}, 2) \geq 150 \) [Elk09] and \( N(\mathbb{Q}, 4) \geq 126 \) [Elk96, Page 9], both due to Elkies. For \( g = 3 \) and \( g \geq 5 \), the current record is \( N(\mathbb{Q}, g) \geq 8g + 16 \), witnessed by Shioda’s curves [Shi98]. Thus, Corollary 1.6 gives a new record for \( N(\mathbb{Q}, g) \) for \( g = 3 \), and for all \( g \geq 5 \) not divisible by 6.

We have \( R(\mathbb{Q}, 1) \geq 19 \) [Elk06] and \( R(\mathbb{Q}, 3) \geq 26 \) [Kul01, Thm. 3.2.1]. The current records \( R(\mathbb{Q}, 2) \geq 32 \) and \( R(\mathbb{Q}, 5) \geq 32 \) have not explicitly appeared in print; the former follows by applying [Kul01, Théorème 2.2.1] to the elliptic curve \( E/\mathbb{Q} \) with \( \text{rk} E/\mathbb{Q} \geq 28 \) found by Elkies [Elk06], which gives genus 2 hyperelliptic curves \( y^2 = f(x) \), with \( \text{deg } f = 6 \). The record for \( g = 5 \) then follows by considering the set of genus 5 curves given by \( y^2 = f(x^2 + bx) \), with \( b \in \mathbb{Q} \); we leave the details to the reader. For \( g = 4 \) and \( g \geq 6 \), the existing record is Shioda’s bound \( R(\mathbb{Q}, g) \geq 4g + 7 \) [Shi98]. Thus, Corollary 1.6 gives a new record for \( R(\mathbb{Q}, g) \) for \( g = 4 \), and for all \( g \geq 7 \) not divisible by 6.

Consider next the constant \( R(\mathbb{Q}, g; Z_2) \). The current record for \( g = 1 \) (elliptic curves) is \( R(\mathbb{Q}, 1; Z_2) \geq 11 \), due to Elkies [Elk07]. For \( g > 2 \), the existing record is \( R(\mathbb{Q}, g; Z_2) > 4g + 2 \), due to Shioda [Shi98, Theorem 7]. Thus, Corollary 1.6 gives a new record for \( R(\mathbb{Q}, g; Z_2) \) for all \( g \) divisible by 3.

Finally, we have \( R(\mathbb{Q}, 1; V_4) \geq 8 \) due to Elkies [Elk07, Page 13]. For \( g \geq 2 \), the bound \( R(k, g; V_4) \geq 4g \) given by Corollary 1.6 appears to be entirely new; we do not know of any construction of large rank curves (even positive rank curves) of genus \( g \geq 2 \) over \( \mathbb{Q} \) with Mordell–Weil group containing \( V_4 \).

Remark 1.9. The constants (1.1) and (1.2) may only increase as \( k \) gets larger, so the bounds in Table 1.7 also hold for any number field \( k \). Of course, Table 1.4 improves these bounds if \( k \) contains cosines or roots of unity not already in \( \mathbb{Q} \); we illustrate this in the case of the quadratic fields \( \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\lambda_{12}) \) and \( \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_6) \). We set \( 2g + 2 = 12d \) in the former case and \( g + 1 = 6d \) in the latter (i.e. we look at the first and last row, respectively, of Table 1.4). Then, Theorem 1.3 yields in the case \( d = 1 \) the bounds \( R(\mathbb{Q}(\sqrt{3}), 5) \geq 40 \) and \( R(\mathbb{Q}(\sqrt{-3}), 5) \geq 36 \); compare these with the published record \( R(k, 5) \geq 32 \) for any number field \( k \) (cf. 1.8). For both of these quadratic fields, the case \( d = 2 \) yields \( R(k, 11) \geq 66 \), and the case \( d \geq 3 \) yields \( R(k, g) \geq 4g + 27 \) for all \( g \geq 17 \) congruent to 5 modulo 6.

When applying Theorem 1.3, instead of fixing \( k \) and allowing \( g \) to vary, we can equally well fix \( g \) and allow \( k \) to vary. From this perspective, Theorem 1.3 almost doubles the existing records for \( R(k, g) \) once \( k \) contains the appropriate cosines or roots of unity. Indeed, taking \( d = 1 \) in Theorem 1.3 yields the following.

Corollary 1.10. For any number field \( k \) and positive integer \( g \), we have

\[
R(k, g) \geq \begin{cases} 
8g & \text{if } k \text{ contains } \lambda_{2g+2}, \lambda_{2g+1}, \text{ or } \lambda_{4g}, \\
8g - 4 & \text{if } k \text{ contains } \zeta_{g+1} \text{ or } \zeta_{2g-1}
\end{cases}
\]

Example 1.11. If \( g \) is even then \( \mathbb{Q}(\lambda_{2g+2}) = \mathbb{Q}(\lambda_{g+1}) \), so in this case Corollary 1.10 gives \( R(k, g) \geq 8g \) if \( k \) contains \( \lambda_{g+1} \). For example, it gives the bounds \( R(k, 6) \geq 48 \) and \( R(k, 8) \geq 64 \) if \( k \) contains the real cubic fields \( \mathbb{Q}(\lambda_1) \) and \( \mathbb{Q}(\lambda_9) \), respectively. For comparison, note that the current published records for any number field \( k \) are \( R(k, 6) \geq 31 \) and \( R(k, 8) \geq 39 \) (cf. 1.8).

1.12. Twist families. The quest for infinitely many genus \( g \) curves over \( k \) with large rank admits a natural counterpart in which we ask for the curves to be pair-wise non-isomorphic over \( k \) but isomorphic over \( \overline{k} \) (recall that two such curves \( X/k \) and \( Y/k \) are then said to be twists of one another). In this direction, the strongest result we know of is due to Mestre. He showed (by way of
a refinement of his own original construction, see Example 5.7) that if \( k \) contains \( \zeta_{2g+2} \), with \( g \) any positive integer, then there exist infinitely many (upto \( k \)-isomorphism) genus \( g \) hyperelliptic curves

\[
T_{a,b}/k : y^2 = ax^{2g+2} + b
\]

having at least \( 16g+1 \) \( k \)-rational points. Our refinement of the Mestre–Shioda construction is in fact a generalization of Mestre’s refinement, and we are also lead to consider these curves \( T_{a,b}/k \), which arise as specializations of the curve \( X_n^{yc} \) from Table 9.3. We are able to go further and show that these points generate rank \( 8g \) in the Jacobian. To state the full result, recall that an abelian variety \( A/k \) has complex multiplication by some number field \( E \) if \( \dim A = [E : Q]/2 \) and there is a \( Q \)-algebra embedding \( E \hookrightarrow \text{End}_k^0(A) := \text{End}_k(A) \otimes \mathbb{Z} Q \).

**Theorem 1.13** (Proved in 15.4). Let \( g \) be a positive integer, and let \( n = 2g + 1 \) or \( 2g + 2 \). Let \( k \) be a number field which contains \( \zeta_n \). Then, there exists a set \( S \subset \mathbb{A}^2(k) \) which is not thin (see 3.3) such that for all \( (a,b) \in S \), the curve \( T_{a,b}/k : y^2 = ax^n + b \) is of genus \( g \) and witnesses the following statements (\( J_{a,b}/k \) denotes the Jacobian of \( T_{a,b}/k \)):

(i) There exists a \( k \)-isogeny of abelian varieties

\[
\Theta : \prod_{m|n, m \geq 3} A_m \longrightarrow J_{a,b},
\]

where each \( A_m/k \) is an abelian variety with complex multiplication by \( Q(\zeta_m) \).

(ii) For all \( m \) dividing \( n \), with \( m \geq 3 \), we have

\[
\text{rk } A_m(k) \geq 4\phi(m) = 8(\dim A_m),
\]

and consequently, we have

\[
\text{rk } T_{a,b}/k \geq 8g.
\]

**1.14.** The curves that witness **Theorem 1.3** are specializations of the curves defined in Table 9.3, which are equipped with many rational points over certain rational function fields (see Table 9.3). Let us here say a few words about these curves in the case \( d = 1 \).

(a) Let \( f_n^{re}(x) \in \mathbb{Z}[x] \) be the polynomial determined by the identity \( f_n^{re}(x + x^{-1}) = x^n + x^{-n} \) (cf. 7.4). That is, \( f_n^{re}(x) = 2T_n(x/2) \), where \( T_n(x) \) is the classical Chebyshev polynomial (of the first kind) which is determined by the functional equation \( T_n(\cos \theta) = \cos(n\theta) \). The bounds in the first three rows of Table 1.4 are witnessed by specializations of the hyperelliptic curves \( X_n^{re} \) and \( \tilde{X}_n^{re} \) in Table 9.3. These specializations are given by equations of the form

\[
C_{a,b}/k : y^2 = af_n^{re}(x) + b, \quad \text{and} \quad \tilde{C}_{a,b}/k : (x + 2)(af_n^{re}(x) + b),
\]

where \( n = 2g + 2 \) or \( 2g + 1 \). The curves \( C_{1,t}/k \) and \( \tilde{C}_{1,t}/k \), for \( t \in k \), are denoted \( C_t \) in the article [TTV91] of Tautz, Top, and Verberkmoes. They show that if \( n = p \) is an odd prime and \( k \) contains \( \lambda_p \), then the Jacobian \( J_t \) of \( C_t \) has real multiplication by \( Q(\lambda_p) \) (i.e. the endomorphism algebra \( \text{End}_k(J_t) \otimes \mathbb{Z} Q \) contains the field \( Q(\lambda_p) \)). In our situation, one can show (but we do not, since it is not directly related to our main goal in this article) that for any \( n \in \mathbb{N} \), the Jacobian of \( C_{a,b} \) has endomorphism algebra containing the product of the fields \( Q(\lambda_m) \), where \( m \) ranges over all divisors of \( n \) greater than 2.

(b) Let \( D_n \) denote the dihedral group of order \( 2n \). The bounds in the last row of Table 1.4 are witnessed by specializations of the hyperelliptic curves \( X_n^{dh} \) (for \( n = g + 1 \) even) and \( \tilde{X}_n^{dh} \) (for \( n = g + 1 \) odd) in Table 9.3. These specializations are given by equations of the form

\[
D_{a,b}/k : y^2 = a(x^{2g+2} + 1) + b x^{g+1}.
\]
This curve is remarkable because, if $k$ contains $\zeta_{g+1}$, then $\text{Aut}_k(\mathcal{D}_{a,b})$ contains a subgroup $H \cong \mathbb{Z}_2 \times D_{g+1}$, with the $\mathbb{Z}_2$ generated by $(x, y) \mapsto (x, -y)$, and the $D_{n}$ generated by the involution $(x, y) \mapsto (1/x, y/x^{g+1})$ together with the $n$-cycle $(x, y) \mapsto (\zeta_{n}x, y)$. Brumer [Cap95, Section 5] established the bound $N(\mathcal{Q}(\zeta_{g+1}), g) \geq 16(g + 1)$ by constructing infinitely many $\mathcal{D}_{a,b}/k$ having $4$ full $H$-orbits $k$-points. Our method similarly yields infinitely many such curves with four full $H$-orbits (note: putting $n = g + 1$ in the last row yields $N = 16g + 16$), but we are able to go one step further and determine that these points generate rank $8g - 4$ in the Jacobian. We remark that, although Brumer’s construction appears to be different from our (i.e. the Mestre–Shioda) construction, we suspect that a suitable change of variables might transform one into the other.

(c) The curve $\mathcal{X}_{n}^{\text{re}}$ (resp. $\tilde{\mathcal{X}}_{n}^{\text{re}}$) mentioned in (a) is closely related to the curve $\mathcal{X}_{n}^{\text{dh}}$ (resp. $\tilde{\mathcal{X}}_{n}^{\text{dh}}$) from (b): the latter arise as a double cover of the former. These covers each give rise to so-called partner curves (see Lemma 10.1 for the definition, and also Proposition 10.5), which are the curves $\mathcal{X}_{n}^{\text{im}}$ and $\tilde{\mathcal{X}}_{n}^{\text{im}}$ in Table 9.3. The specializations of $\mathcal{X}_{n}^{\text{im}}$ witness the bounds in the second-last row of Table 1.4; they are given by equations of the form

$$B_{a,b}/k : y^2 = (x^2 - 4)(af_{n}^{\text{re}}(x) + b),$$

where $n = 2g - 1$. The copy of $V_4$ in the Jacobian is generated by the divisor classes $[(2,0) - \infty]$ and $[(-2,0) - \infty]$.

**Remark 1.15.** The analogues of Faltings’ Theorem and the Mordell-Weil Theorem also hold for curves $X/K$, with $K$ the function field of a variety over a finite field $\mathbb{F}_q$. It is proved in [CUV12] (resp. [Ulm07]) that $N(\mathbb{F}_q(t), g) = \infty$ (resp. $R(\mathbb{F}_q(t), g) = \infty$); this automatically implies that the same is true if we replace $\mathbb{F}_q(t)$ with any function field over $\mathbb{F}_q$.

1.16. **Outline of the article.** In Section 2 we develop some tools for determining when a collection of points on a hyperelliptic curve generate a group of large rank in the Jacobian. In Section 3 we review the specialization method alluded to in the introduction. In Section 4 we outline the Mestre–Shioda Construction, and in Section 5 our basic strategy for refining the construction to get better bounds.

The strategy requires us to understand when the splitting fields $\mathbb{K}_f/\mathbb{K}$ of certain composite polynomials $m(f(x)) \in \mathbb{K}[x]$ are rational function fields over $k$ (here, $\mathbb{K}$ is a field showing up in Mestre’s construction). We answer this question after giving an explicit construction of $\mathbb{K}_f$ in Section 6. The answer implies, among other things, that the monodromy group of $f(x)$, defined in 6.3, must be a finite subgroup of $\text{PGL}_2(k)$. It is this requirement that ultimately leads to the various conditions $\lambda_{n} \in k$ and $\zeta_{n} \in k$ present in Theorem 1.3; see 7.1. The curves which witness the theorem are all hyperelliptic curves given by an equation of the form $y^2 = q(x)h(f(x))$, where $h$ is of degree $d$, $f$ is of degree $n$, and $q$ is of degree at most $2$ (hence the title of the article). In Theorem 1.3, the restrictions on the genera are essentially a consequence of the genus-degree formula for hyperelliptic curves.

In Section 7, we consider $f_{n}^{\text{re}}(x)$ (mentioned in 1.14) and other closely related polynomials for which $\mathbb{K}_f$ (constructed explicitly in Section 8 following the method in Section 6) is a rational function field over $k$. Then, in Section 9 we define eight families of curves following the idea of Section 5. These curves come equipped with many rational points over the associated fields $\mathbb{K}_f$. We define certain subgroups $W_n^{\text{*}}$ (in the Jacobian) associated to the points, and state in Theorem 9.17 a “main” theorem giving point and rank bounds for the curves. We utilize this main theorem to give the proof of Theorem 1.3 in 9.20 (deferring to Section 14 the proof that certain curves over function fields are non-isotrivial).
We outline in 9.19 our overall strategy for bounding the ranks of the eight families of curves. The first step is a reduction step which allows us to reduce our consideration to three of the families; this is carried out in Section 10. The next step consists first in fitting the curves together, by making use of some beautiful (and fairly intricate) polynomial identities, into inverse systems indexed by \( n \in \mathbb{N} \) (see Section 11). These inverse systems give rise to various isogeny decompositions and relations between the respective Jacobians (which are possibly of independent interest and worth further exploration). In Section 12, we exploit these decompositions to reduce our task (of determining the ranks of the groups \( W_n^* \)) to determining the rank of certain distinguished subgroups \( V_n^* \subseteq W_n^* \). We accomplish this in Section 13 by bringing to bear the tools from Section 2. Finally, in Section 15 we use Theorem 9.17 to prove Theorem 1.13.

1.17. Acknowledgements. This work is an extension of Chapter One of the author’s PhD Thesis at the University of Georgia. The author is indebted to his PhD advisor Dino Lorenzini for his careful reading and thoughtful feedback on an earlier draft of this work. The author would like to thank Doug Ulmer for several useful discussions on the present draft, and in particular, for his help in clarifying some ideas behind Section 11. The author gratefully acknowledges the support of the Department of Mathematics at the University of Georgia as well as at the University of Arizona in providing a stimulating environment for research.

2. Tools for bounding ranks of hyperelliptic curves

2.1. Notation and Conventions. Let \( k \) be a field. We call a scheme \( X/k \) a \( k \)-variety if \( X \) is geometrically integral, separated, and of finite type over \( k \). In this case the function field of \( X \) is denoted \( k(X) \), and for a finite extension \( \ell/k \), the function field of the base-change \( X \times_k \ell \) is denoted \( \ell(X) \). We call a morphism \( \pi : X \rightarrow Y \) of \( k \)-varieties a cover if it is finite and surjective. The degree of the cover is as usual the degree of the induced function field extension \( k(X)/k(Y) \).

We use bold font as short-hand to denote tuples of indeterminates; for instance, if we say “\( t \) denotes the tuple of indeterminates \( t_1, \ldots, t_n \),” then \( k[t] \) denotes \( k[t_1, \ldots, t_n] \), \( K(t) \) the function field \( K(t_1, \ldots, t_n) \), and \( \mathbb{A}^n_k \) the affine space \( \text{Spec} k[t] \).

We call a field extension \( \ell/k \) Galois if it is algebraic, separable, and normal, and we denote its Galois group \( \text{Aut}_k(\ell) \) by \( \text{Gal}(\ell/k) \). We call \( \ell/k \) a splitting field of a polynomial \( f(x) \in k[x] \) if \( f \) factors completely in \( \ell[x] \) and \( \ell \) is generated as \( k \)-algebra by the roots of \( f \).

2.2. Curves and Jacobians. We call a curve \( X/k \) a nice curve if it is smooth, projective, and geometrically integral. We denote by \( \text{Div}(X) \) the group of divisors on \( X \), \( \text{Div}^0(X) \) the divisors of degree 0, and \( \text{Pic}^0(X) \) the group of degree 0 divisors modulo principal divisors. We denote the Jacobian of \( X/k \) by \( J_X/k \); recall that this is an abelian variety of dimension \( g \) (the genus of \( X \)) such that \( J_X(\ell) \cong \text{Pic}^0(X\ell) \) for any field extension \( \ell/k \) that verifies the condition \( X(\ell) \neq \emptyset \).

2.3. Hyperelliptic curves. By a hyperelliptic curve over a field \( K \), we mean a nice curve \( X/K \) which admits an involution \( \iota \in \text{Aut}_K(X) \) such that the quotient by \( \iota \) is a double cover \( \pi : X \rightarrow \mathbb{P}^1_k \); contrary to the convention in the literature, we do not require that the genus of \( X \) be at least 2. This introduces a slight ambiguity in that the double cover \( \pi \) is unique (up to choosing a coordinate on \( \mathbb{P}^1_k \)) if and only if \( g \geq 2 \). In practice, we will typically work with hyperelliptic curves given by an explicit equation \( X/K : y^2 = f(x) \), for some separable polynomial \( f(x) \in k[x] \) of degree \( d \geq 1 \) (this notation means \( X/K \) is the smooth proper model of the affine plane curve defined by \( y^2 = f(x) \)). In this case, \( \iota \) will always denote the involution \( (x, y) \mapsto (x, -y) \), and \( \pi : X \rightarrow \mathbb{P}^1_k \) the double cover \( (x, y) \mapsto x \). We denote by \( D_\infty \) the degree 2 divisor \( \pi^* \infty \subseteq X \). The genus \( g \) of \( X \) is determined by the formula \( d = 2g + 1 \) or \( d = 2g + 2 \), depending on the parity of \( d \).
2.4. Setup. Let \( L/K \) be an extension of perfect fields of characteristic different from 2, let \( g \) be a positive integer, and let \( X/K \) be a genus \( g \) hyperelliptic curve with Jacobian denoted \( J/K \). We fix an involution \( \iota \in \text{Aut}_K(X) \) whose quotient is a double cover \( \pi : X \rightarrow \mathbb{P}^1_K \). This data will remain fixed until the end of this section.

In Lemma 2.12 below, we give sufficient conditions for a collection of \( L \)-points on \( X \) to generate a group of large rank in the Jacobian. The main geometric tool we use is Lemma 2.6. This is an immediate consequence of the Castelnuovo–Severi Inequality (see [ACGH85, Page 366] or [Sti84, Satz 1]), which says the following.

Suppose \( C, C_1, \text{ and } C_2 \) are nice curves over \( K \) and \( \varphi_1 : C \rightarrow C_1 \) and \( \varphi_2 : C \rightarrow C_2 \) are covers which do not factor through a mutual cover \( C \rightarrow \overline{C} \). Then, writing \( d_i \) for the degree of \( \varphi_i \), the genera of the curves satisfy the inequality

\[
g(C) \leq g(C_1)(d_2 - 1) + g(C_2)(d_1 - 1) + (d_2 - 1)(d_1 - 1). \tag{2.5}
\]

**Lemma 2.6.** Let \( \mathcal{D} \in \text{Div}^0(X_L) \) be a reduced divisor such that (i) \( \mathcal{D} \neq 0 \) \( \mathcal{D} \) and (ii) the support of \( \mathcal{D} \) consists of at most \( 2g \) geometric points of \( X \). Then \( \mathcal{D} \) is a non-zero point of \( J(L) \).

**Proof.** Assume for a contradiction that \( \mathcal{D} \) is the divisor of a rational function \( \psi \) on \( X_L \). Assumption (i) implies that the cover \( \psi : X_L \rightarrow \mathbb{P}^1_L \) does not factor through the double cover \( \pi : X_L \rightarrow \mathbb{P}^1_L \), and assumption (ii) implies that \( g \geq \deg \psi \). If we take \( C \) to be \( X, C_1 \) and \( C_2 \) to both be \( \mathbb{P}^1_L \), and the \( \varphi_1 \) and \( \varphi_2 \) to be \( \pi \) and \( \psi \), then the Castelnuovo–Severi Inequality (2.5) reads \( g \leq (\deg \psi) - 1 \), which is a contradiction. \( \square \)

2.7. Fix an integer \( n \geq 2 \), and let \( G \subset \text{Aut}_K(L) \) be a cyclic subgroup generated by an automorphism \( \sigma \) of order \( n \). Let \( P \) be an \( L \)-rational point of \( X \) which **generates a \( G \)-torsor**; by this, we mean that the \( G \)-orbit \( \{ P, \alpha P, \ldots, \sigma P \} \subset X(L) \) is of size \( n \) (and is hence a \( G \)-torsor). Viewing \( \text{Div} X_L \) as a \( \mathbb{Z}G \)-module, this amounts to saying that the submodule

\[
W := \text{span}_{\mathbb{Z}G}\{ P \} \subset \text{Div}(X_L)
\]

is free of rank one over \( \mathbb{Z}G \). Let \( \Phi_n(x) \in \mathbb{Z}[x] \) denote the \( n \)-th cyclotomic polynomial; recall that \( \Phi_n(x) \) is irreducible over \( \mathbb{Z} \), since its roots are the primitive \( n \)-th roots of unity, and the degree of \( \Phi_n \) is the Euler Totient \( \phi(n) \). The \( n \)-th **inverse cyclotomic polynomial** is defined by

\[
\Psi_n(x) := \frac{x^n - 1}{\Phi_n(x)} \in \mathbb{Z}[x]. \tag{2.8}
\]

Any divisor \( D \in W \) can be written in the form \( D = q(\sigma)P \) for some polynomial \( q(x) \in \mathbb{Z}[x] \), and the degree of such a divisor is the integer \( q(1) \). Since \( \Psi_n(1) = 0 \), the divisor \( \mathfrak{P} := \Psi_n(\sigma)P \in W \) is of degree 0, and we may consider the \( \mathbb{Z}G \)-modules

\[
V := \text{span}_{\mathbb{Z}G}\{ \mathfrak{P} \} \subset \text{Div}^0 X_L,
\]

\[
[V] := \text{span}_{\mathbb{Z}G}\{ [\mathfrak{P}] \} \subset J(L). \tag{2.9}
\]

Identifying the group ring \( \mathbb{Z}G \) with the commutative ring \( \mathbb{Z}[\sigma]/(\sigma^n - 1) \), we have the following.

**Lemma 2.10.** The map \( \mathbb{Z}G \rightarrow \text{End}(V) \) factors through the natural quotient

\[
\mathbb{Z}G \rightarrow \mathbb{Z}[\xi_n], \quad \sigma \mapsto \xi_n := e^{2\pi i/n}
\]

to give an embedding \( \mathbb{Z}[\xi_n] \hookrightarrow \text{End}(V) \). In this way, \( V \) is a free \( \mathbb{Z}[\xi_n] \)-module of rank one, and \([V] \) verifies one of the following two statements, depending on the order of \([\mathfrak{P}] \in J(L) \).

\((a)\) \([\mathfrak{P}] \) is torsion; in this case \([V]_{\mathbb{Q}} := [V] \otimes_{\mathbb{Z}} \mathbb{Q} = 0.\)
(b) \([\mathfrak{P}]\) is of infinite order; in this case \([V]_Q\) is a free \(Q(\zeta_n)\)-module of rank one, and hence, \(\dim_Q[V]_Q = \phi(n)\).

**Proof.** Using that \(W\) is free of rank one over \(ZG\), for any element \(f(\sigma)\mathfrak{P} \in V\), we have \(f(\sigma)\mathfrak{P} = f(\sigma)\Psi_n(\sigma)P = 0 \in V\) if and only if \(x^n - 1\) divides \(f(x)\Psi_n(x)\) in \(Z[x]\), which holds if and only if \(\Phi_n(x)\) divides \(f(x)\) in \(Z[x]\). It follows that the kernel of the ring homomorphism \(ZG \rightarrow \text{End}(V_n)\) is generated by \(\Phi_n(\sigma)\), so it factors through the quotient \(Z[\zeta_n] = ZG/\Phi_n(\sigma)\) to give an embedding \(Z[\zeta_n] \hookrightarrow \text{End}(V)\). We have a natural surjection of \(ZG\)-modules \([-] : V \twoheadrightarrow [V]\) defined by \(E \mapsto [E]\), and since \(\Phi(\sigma)\) annihilates \(V\), it also annihilates \([V]\). Thus, \([V]_Q\) is a \(Q(\zeta_n)\)-module generated by \([\mathfrak{P}]\), which immediately implies that one of the statements, (a) or (b), holds. \(\square\)

In the next lemma, we give sufficient conditions for the point \([\mathfrak{P}]\) to be of infinite order. The main idea is to produce a distinguished divisor \(D \subset X(L)\) satisfying the conditions of Lemma 2.6 such that, if \([\mathfrak{P}]\) were torsion, then \([D] = 0 \in J(L)\), contradicting Lemma 2.6. To make this work, we require that the torsion subgroup of \(J(L)\) be bounded (in the sense of (a2)), and that \(g\) be sufficiently large relative to \(n\). Define the integer

\[
\|n\| := \text{the number of distinct prime factors of } n. \tag{2.11}
\]

**Lemma 2.12.** Continuing with 2.7 above, assume that the following hold.

(a1) \(P\) and \(\iota P\) generate \(G\)-torsors which are disjoint in \(X(L)\).

(a2) We have an equality of torsion subgroups \(J(L)_{\text{tors}} = J(K)_{\text{tors}}\).

(a3) The genus \(g\) of \(X\) satisfies \(g \geq \max\{2, 2\|n\|^{-1}\}\) (in particular, \(g \geq 2\)).

Then \([V] \subset J(L)\) is a free abelian group of rank \(\phi(n)\) (i.e. statement (b) of Lemma 2.10 holds).

**Proof.** Assume for a contradiction that \([\mathfrak{P}]\) is a torsion point. We proceed in two separate cases.

(i) \(\|n\| = 1\). In this case, (a3) says that \(g \geq 2\), and hence, that \(4 \leq 2g\). We have \(n = p^e\) for some prime \(p\) positive integer \(e\), so \(\mathfrak{P}\) is the divisor \((\sigma^n/p - 1)P\). Define

\[
\mathfrak{D} := (\sigma - 1)\mathfrak{P} = (\sigma^{\frac{n}{p}+1}P + P) - (\sigma^\frac{n}{p}P + \sigma P) \in V.
\]

Then (a1) implies that \(\mathfrak{D}\) is a reduced divisor with support consisting of 4 points, and that \(\mathfrak{D} \neq \iota\mathfrak{D}\), so Lemma 2.6 implies \([\mathfrak{D}] \neq 0 \in J(L)\). But (a2) forces \([\mathfrak{D}] = (\sigma - 1)[\mathfrak{P}] = 0 \in J(L)\), a contradiction.

(ii) \(\|n\| > 1\). In this case (a3) says that \(2\|n\| \leq 2g\). Assumption (a2) implies that \((1 - \zeta_n)\) annihilates the \(Z[\zeta_n]\)-module \([V]\). Since \(n\) is composite, \((1 - \zeta_n)\) is a unit in \(Z[\zeta_n]\), so \([V] = \{0\} \subset J(L)\). Define now the polynomial and divisor

\[
\tilde{\Psi}_n(x) := \prod_{p \text{ prime}, p|n} (x^\frac{n}{p} - 1) \in Z[x], \quad \mathfrak{D} := \tilde{\Psi}_n(\sigma)P \in \text{Div}^0(X_L).
\]

Since \(\Psi_n(x)\) divides \(\tilde{\Psi}_n(x)\) in \(Z[x]\), the point \([\mathfrak{D}] \in J(L)\) lies in \([V]\), so we have \([\mathfrak{D}] = 0 \in J(L)\). Let \(\mathcal{P}\) denote the set of primes dividing \(n\). For any subset \(S \subset \mathcal{P}\), define

\[
\sigma_S := \prod_{p \in S} \sigma^{n/p} \in G,
\]

so that

\[
\mathfrak{D} = \sum_{S \subset \mathcal{P}} (-1)^{\|n\|-\#S} \sigma_S P \in \text{Div}^0(X_L).
\]

Each element \(\sigma^{n/p} \in G\) is of order \(p\), so each element \(\sigma_S\) is of order \(\prod_{p \in S} p\). This implies that the \(2\|n\|\) elements \(\{\sigma_S \in G\}_{S \subset \mathcal{P}}\) are pair-wise distinct. Then, (a1) implies that \(\mathfrak{D} \neq \iota\mathfrak{D}\), and that
\( \mathcal{D} \) is reduced with support consisting of the \( 2^{[n]} \) points \( \{ \sigma_s P \}_{S \subset P} \). But Lemma 2.6 implies that \( [\mathcal{D}] \neq 0 \in J(L) \), a contradiction.

2.13. In Section 9 we define certain hyperelliptic curves over rational function fields, and in Table 9.3 we exhibit tuples of rational points on these curves. Lemma 2.12 turns out to be a robust tool for determining the corresponding subgroups generated in the respective Mordell–Weil groups; we use it to dispense with all the cases in which the curves in question are of genus at least 2 (see the proof of Theorem 13.1). This is a consequence of two pleasant features of the Mestre–Shioda construction (cf. 4.4 and 5.1). The first is that these points enjoy a high degree of symmetry, namely, they generate torsors under cyclic groups (exactly as in Lemma 12.3 above). The second is that they are transcendental points of the curves (we call a point \( P : \text{Spec} \ L \to X \) transcendental if the image of \( P \) is the generic point of \( X \)). We conclude this section with two lemmas which exploit this last feature—Lemma 2.14 is used to obtain the assumption (a2) in Lemma 2.12, and Lemma 2.15 is used in the proof of Theorem 13.1 to deal with the genus one cases.

**Lemma 2.14.** If \( K \) is algebraically closed in \( L \), then we have an equality of torsion subgroups 
\[
J(L)_{\text{tors}} = J(K)_{\text{tors}}.
\]

**Proof.** Suppose \( P : \text{Spec} \ L \to J \) is a torsion point of order \( n \), and let \( x \in J \) be the image of \( P \). Then \( x \) lies in \( J[n] \), the kernel of multiplication by \( n \). Since \( J[n] \) is a finite \( K \)-scheme, the residue field \( \kappa(x) \) is a finite extension of \( K \). The morphism \( P : \text{Spec} \ L \to \text{Spec} \kappa(x) \) gives a \( K \)-algebra inclusion \( \kappa(x) \hookrightarrow L \). So, if \( K \) is algebraically closed in \( L \) then \( \kappa(x) = K \) and we conclude that \( P \in J(K)_{\text{tors}} \) (more precisely, that \( P \) is the base-change to \( L \) of the point \( x \in J(K)_{\text{tors}} \)).

**Lemma 2.15.** Let \( P \in X(L) \) be a transcendental point, and let \( D \in \text{Div} \ X \) be an effective divisor of degree \( d \geq 1 \). Then, the point \([dP - D] \in J(L)\) is of infinite order.

**Proof.** Put \( \mathcal{D} := dP - D \), and assume for a contradiction that \( [\mathcal{D}] \) is a torsion point of \( J(L) \). If \( n \) denotes the order of this point, then by replacing \( d \) (resp. \( D \)) with \( nd \) (resp. \( nD \)), we may assume for a contradiction simply that \( [\mathcal{D}] = 0 \in J(L) \). Recall that the \( d \)-th symmetric power of \( X/K \) is a variety \( X^{(d)}/K \) whose \( F \)-points (for any extension \( F/K \)) are naturally in bijection with the effective degree \( d \) divisors on \( X_F \). Consider the \( K \)-morphism \( j : X \to J \) defined as the composition of the \( K \)-morphisms 
\[
X \xleftarrow{\Delta} X^d \xrightarrow{\cdot d} X^{(d)} \xrightarrow{\cdot d} J,
\]
where the first arrow is the diagonal embedding, the second is the natural quotient by the symmetric group \( S_d \), and the last arrow is defined on \( F \)-points (for any \( L/K \)) by \( E \mapsto [E - D] \). Thus, for any point \( Q \in X(L) \), we have \( j(Q) = [dQ - D] \). Since the morphism \( j : X \to J \) is non-constant, the image of the composition \( j \circ P : \text{Spec} \ L \to J \) is not a closed point. But this is absurd since \( j(P) = [\mathcal{D}] = 0 \in J(L) \).

3. The specialization method

In this section, \( k \) denotes an infinite, finitely generated field (i.e., field).

**3.1. Non-isotrivial curves.** Let \( \mathbb{K}/k \) be the function field of a \( k \)-variety \( \mathbb{V} \) of positive dimension, and let \( \mathbb{X}/\mathbb{K} \) be a nice curve of positive genus. We say that \( \mathbb{X}/\mathbb{K} \) is constant if there is an \( \mathbb{K} \)-isomorphism \( \mathbb{X} \cong X_{\mathbb{K}} \) for some curve \( X/k \). We say that \( \mathbb{X}/\mathbb{K} \) is isotrivial if \( \mathbb{X}_{\mathbb{L}}/\mathbb{L} \) is constant, for some finite extension \( \mathbb{L}/\mathbb{K} \). By replacing \( \mathbb{V} \) with an open subset if necessary, we can spread out \( \mathbb{X}/\mathbb{K} \) to a smooth, projective family of curves \( \mathbb{X} \to \mathbb{V} \) with geometrically integral fibers.
Proof. Part (b) follows by applying Theorem 3.4 to the relative Jacobian $N/V$ because, after replacing set $S$ thin set $V$ Hilbert Property (see [Ser97, Section 9.5, Page 129]), so if curves $X/K$ group. Let Corollary 3.5. is thin. In particular, if $V/K$ is not thin for every $V/k$, then implies that: $V(k)/V$ is thin if and only this morphism $X/K$ is a Hilbertian if $P^n(k)$ is not thin for every $n \geq 1$. It is known (see [Ser97, Section 9.5, Page 129]) that ifg fields (in particular, number fields) are Hilbertian.

Theorem 3.4 ([CT20, Theorem 2.4], [Ser97, Section 11.1]). Let $V$ be a smooth $k$-variety with function field $K$, and let $J/V$ an abelian scheme with generic fiber $J/K$. Then, the set

$$T := \{ P \in V(k) \mid \sigma_P : J(K) \to J_P(k) \text{ is not injective} \}$$

is thin. In particular, if $V/k$ satisfies the Hilbert Property, then $V(k) \setminus T$ is Zariski-dense in $V$.

Recall the constants defined in (1.1) and (1.2).

Corollary 3.5. Let $k$ be an i.f.g. field, let $R$ and $N$ be positive integers, and let $B$ be a finite abelian group. Let $K/k$ be a rational function field, and $X/K$ a non-isotrivial curve of genus $g \geq 1$.

(a) If $\#X(K) \geq N$, then $N(k, g) \geq N$.

(b) If $J(K)$ contains a subgroup isomorphic to $B \oplus Z^R$, then $R(k, g; B) \geq R$.

Proof. Choose a smooth $k$-variety $V$ with function field $K$ which admits a smooth, projective family of curves $X/V$ with generic fiber $X/K$ (as in 3.1). Since $V$ is a $k$-rational variety, it satisfies the Hilbert Property (see [Ser97, Section 9.5, Page 129]), so $V(k) \setminus S$ is Zariski-dense in $V$ for any thin set $S \subset V(k)$. The non-isotriviality of $X/K$ then implies that: if $S \subset V(k)$ is thin, then the set $\{X_P/k\}_{P \in V(k) \setminus S}$ contains infinitely many nice genus $g$ curves over $k$. Now, part (a) follows because, after replacing $V$ with a suitable open subset, any $N$ points of $X(K)$ can be spread out to $N$ disjoint sections $V \to X$ (i.e. they specialize to $N$ distinct $k$-points on any $k$-fiber of $X/V$). Part (b) follows by applying Theorem 3.4 to the relative Jacobian $J/V$ of $X/V$.

4. The Mestre–Shioda Construction

In this section, and continuing until the end of 6.13, $k$ denotes a field of characteristic different from 2. The Mestre–Shioda construction is predicated on the following lemma. For the rest of the
Then, the map $k[œ] \rightarrow k[œ]$. This homomorphism is injective and gives the factorization

Thus, if $k$ is an i.f.g. field (cf. Section 3) then we can apply Corollary 3.5 to get the bounds $N(k, g) \geq 8g + 12$ and $R(k, g) \geq 4g + 5$. 

**Lemma 4.1.** Let $m, q,$ and $h$ denote the tuples of indeterminates $m_0, \ldots, m_{2d+1}, q_0, \ldots, q_d,$ and $h_0, \ldots, h_d,$ respectively. Define the polynomials

$$
\begin{align*}
m(x) &:= x^{2d+2} + m_{2d+1}x^{2d+1} + \cdots + m_0 \in k[m][x], \\
q(x) &:= x^{d+1} + q_d x^{d} + \cdots + q_0 \in k[q][x], \\
h(x) &:= h_d x^{d} + \cdots + h_0 \in k[h][x].
\end{align*}
$$

(4.2)

Then, the map $k[m] \rightarrow k[h, q]$ defined by equating coefficients in the identity

$${m(x) = q(x)^2 - h(x)}$$

(4.3)

is a $k$-algebra isomorphism.

**Proof.** One can express each $q_i, h_i$ as a polynomial in the variables $m_0, \ldots, m_{2d-1}$ by comparing coefficients (in descending order) in the identity $m(x) = q(x)^2 - h(x)$ and sequentially solving for the variables $q_d, \ldots, q_0, h_d, \ldots, h_0$; we leave the details to the reader. \hfill \Box

4.4. Identifying $k[m]$ with $k[h, q]$ via the isomorphism in Lemma 4.1, we view $h(x), q(x)$ and $m(x)$ as polynomials in $k[m][x]$ satisfying the identity (4.3). Let $u$ denote the tuple of indeterminates $u_1, \ldots, u_r,$ let $s_i(u)$ denote the $i$-th elementary symmetric function in $u,$ and define the $k$-algebra homomorphism

$$
k[m] \hookrightarrow k[u], \quad m_i \mapsto (-1)^i s_{r-i}(u), \quad \text{for } i = 0, \ldots, r - 1.
$$

(4.5)

This homomorphism is injective and gives the factorization

$$
m(x) = (x - u_1) \cdots (x - u_r) \in k[u][x].
$$

(4.6)

Put $M := k(m)$ and $K := k(u),$ and define the $(d + 1)$-dimensional rational function field

$$
K := k(h) = k(h_0, \ldots, h_d),
$$

so that we have a chain of (transcendental) field extensions $k \hookrightarrow K \hookrightarrow K.$ Now, Mestre’s construction [Mes91a, Mes91b] extracts from the identities (4.3) and (4.6) the following geometric consequence: the hyperelliptic curve

$$
X/K : y^2 = h(x)
$$

has the $K$-rational points

$$
Q_i := (u_i, q(u_i)), \quad \text{for } i = 1, \ldots, r.
$$

(4.7)

These points, together with their conjugates $iQ_i = (u_i, -q(u_i)),$ contribute $2r = 4d + 4$ $K$-points to $X.$ For $i = 1, \ldots, r,$ define the divisor $\sigma_i := 2Q_i - D_\infty \in \text{Div}^0(X_K)$ (cf. 2.3). Then, we have

$$
2\text{div}(y - q(x)) = \sigma_1 + \cdots + \sigma_r \in \text{Div}^0(X_K),
$$

giving the relation $[\sigma_1] + \cdots + [\sigma_{2d+2}] = 0 \in J(K),$ where $J/K$ denotes the Jacobian of $X.$ Shioda showed in [Shi98, Theorems 4, 5] that if $g$ is positive (i.e. if $d \geq 3$), then the points $[\sigma_i]$ do not satisfy any other relation and hence generate a subgroup of rank $r - 1 = 2d + 1$ in $J(K).$

Now, if $d$ is even then the genus $g$ of $X$ satisfies $d = 2g + 2,$ so we have the bounds

$$
#X(K) \geq 2r = 8g + 12 \quad \text{and} \quad \text{rk } X/K \geq 4g + 5.
$$

(4.8)

Thus, if $k$ is an i.f.g. field (cf. Section 3) then we can apply Corollary 3.5 to get the bounds $N(k, g) \geq 8g + 12$ and $R(k, g) \geq 4g + 5.$
5. STRATEGY BEHIND IMPROVEMENT

5.1. Let \( f(x) \in k[x] \) be a polynomial of degree \( n \geq 1 \). Our basic idea, generalizing Example 5.7 below, is to consider (variants of) the hyperelliptic curve
\[
\mathbb{X}_f / K : \ y^2 = \mathbb{h}(f(x)).
\]
This curve fits into a commutative diagram:
\[
\begin{array}{ccc}
\mathbb{X}_f & \xrightarrow{\phi_f} & \mathbb{X} \\
\downarrow \pi & & \downarrow \pi \\
\mathbb{P}^1_K & \xrightarrow{f} & \mathbb{P}^1_K.
\end{array}
\]  
(5.2)

To simplify the exposition, suppose for the moment that \( nd \) is even. Then, since \( \mathbb{h}(f(x)) \) is separable (cf. Lemma 6.1), the genus \( g_f \) of \( \mathbb{X}_f \) is determined by the formula
\[
nd = 2g_f + 2, \tag{5.3}
\]
Let \( \mathbb{K}_f / \mathbb{K} \) be a splitting field extension for \( \mathfrak{m}(f(x)) \). One checks, by replacing \( x \) with \( f(x) \) in (4.3), that \( \mathbb{X}_f \) has the \( \mathbb{K}_f \)-points
\[
\{ Q_t := (t, q(f(t))) \mid \mathfrak{m}(f(t)) = 0 \}. \tag{5.4}
\]
Since \( \mathfrak{m}(f(x)) \) has \( rn \) distinct roots \( t \in \mathbb{K}_f \) (cf. Lemma 6.1), the points (5.4) and their hyperelliptic conjugates \( tQ_t := (t, -q(f(t))) \) yield
\[
\#\mathbb{X}_f(\mathbb{K}_f) \geq 2rn = 8g_f + 4n + 8. \tag{5.5}
\]
Fixing any root \( t \) of \( \mathfrak{m}(f(x)) \) and letting \( t' \) vary over the remaining roots, we have \( rn - 1 \) points \( [Q_t - Q_{t'}] \in \mathbb{J}_f(\mathbb{K}_f) \). If these are linearly independent, then we have
\[
\text{rk} \mathbb{X}_f / \mathbb{K}_f \geq rn - 1 = 4g_f + 2n + 3. \tag{5.6}
\]
The key observation now is that, relative to \( g_f \), the number of \( \mathbb{K}_f \)-points constructed grows linearly in \( n \). Indeed, if \( f(x) = x \) (so that \( n = 1 \) and \( d = 2g_f + 2 \), then we have \( \mathbb{X}_f = \mathbb{X} \) and \( \mathbb{K}_f = \mathbb{K} \), and (5.5) and (5.6) specialize to the bounds in (4.8). At the other extreme, if \( d = 1 \) and \( n = 2g_f + 2 \), then (5.5) and (5.6) would give lower bounds
\[
\#\mathbb{X}_f(\mathbb{K}_f) \geq 16g_f + 16 \quad \text{and} \quad \text{rk} \mathbb{X}_f / \mathbb{K}_f \geq 8g_f + 7. \tag{5.7}
\]
Supposing we are able to get a good rank bound, we would like to then specialize \( \mathbb{X}_f / \mathbb{K}_f \) (by applying Theorem 3.4) to obtain curves over \( k \) with large rank. Thus, the usefulness of our strategy is tempered by the requirement that \( \mathbb{K}_f \) must be the function field of a \( k \)-variety which satisfies the Hilbert Property (cf. 3.3). We examine when this holds in the next section.

Example 5.7. The observation that curves of the form \( \mathbb{X}_f \) have more points relative to genus (than Mestre’s “original” curve \( \mathbb{X} \)) was inspired by the following antecedents in the literature.

(a) In [Shi98], Shioda worked with the case \( f(x) = x^2 \), so that \( n = 2 \). The curve \( \mathbb{X}_f / K : y^2 = \mathbb{h}(x^2) \) is non-constant of genus \( g_f = d - 1 \), and Shioda proved that the inequality (5.6) holds if \( g_f \geq 2 \). The splitting field \( \mathbb{K}_f \) of \( \mathfrak{m}(x^2) \in \mathfrak{m}[x] \) is a rational function field over \( k \) (see

\[1\]

\[1\]It turns out, in all the cases we consider, that the classes \( [Q_t - Q_{t'}] \in \mathbb{J}_f(\mathbb{K}) \) associated to the points (5.4) never generate rank greater than \( 8g_f \). This occurs because the \( K \)-morphism \( \phi_f : \mathbb{X}_f \to \mathbb{X} \cong \mathbb{P}^1_K \) introduces linear dependence relations of the form \( [\phi_f^* E] = 0 \in \mathbb{J}_f(\mathbb{K}) \), where \( E \) is a degree zero divisor on \( \mathbb{P}^1_K \).
Example 6.10), so the Specialization Theorem 3.4 yields the bounds \( R(k, g_f) \geq 4g_f + 7 \) and \( N(k, g_f) \geq 8g_f + 16 \) (which constitute the current published records for large enough \( g \)).

(b) Mestre (see [Elk96, Page 4]) considered the case \( d = 1 \) and \( f(x) = x^{2g+2} \). He observed that \( \mathbb{K}_f/K : y^2 = h_1x^{2g+2} + h_0 \) is a genus \( g \) curve having at least \( 16(g + 1) \) rational points over \( \mathbb{K}_f \), which is again a rational function field over \( k \) (in fact, \( \mathbb{K}_f \) is the field \( \mathbb{K}^{\text{cyc}}_n \) defined in 8.2).

6. Constructing the Splitting Field \( \mathbb{K}_f \) of \( \mathfrak{m}(f(x)) \) over \( \mathbb{K} \)

We fix for this section a polynomial \( f(x) \in \mathbb{K}[x] \) of degree \( n \geq 1 \). In 6.6 below, we construct an abstract splitting field extension \( \mathbb{K}_f \) for the composition \( \mathfrak{m}(f(x)) \in \mathbb{K}[x] \) (under a simplifying assumption on \( f \)). In Proposition 6.11 we give necessary and sufficient conditions (in terms of a certain curve \( C_f/k \) associated to \( f \)) for \( \mathbb{K}_f \) to be a rational function field over \( k \). Lemma 6.15 furnishes a key ingredient in determining the ranks of our curves.

Lemma 6.1. Let \( f(x) \in \mathbb{K}[x] \) be a polynomial of degree \( n \geq 1 \) whose derivative \( f'(x) \) is not identically zero. Let \( \mathbf{g} \) denote the tuple \( g_0, \ldots, g_{r-1}, \) with \( r \geq 1 \), and define

\[
g(x) := x^r + g_{r-1}x^{r-1} + \cdots + g_0 \in \mathbb{K}[\mathbf{g}][x].
\]

Then, the composition \( \mathbf{g}(f(x)) \in \mathbb{K}[\mathbf{g}][x] \) is irreducible and separable. Moreover, the set of irreducible factors of \( \text{disc}(\mathbf{g} \circ f) \) in \( \mathbb{K}[\mathbf{g}] \) (up to scaling by \( \mathbb{K}^\times \)) is

\[
\{\text{disc} \mathbf{g} \} \cup \{\mathbf{g}(f(\alpha)) \mid f'(\alpha) = 0\}.
\]

Proof. We assume without loss of generality that \( \mathbb{K} \) is algebraically closed. Let \( \mathbb{K}(\mathbf{g}) \hookrightarrow \mathbb{K}(\mathbf{v}) = K(v_1, \ldots, v_r) \) be the injection which gives the factorization \( \mathbf{g}(x) = (x-v_1) \cdots (x-v_r) \in \mathbb{K}(\mathbf{v})[x] \), so that we have the factorization \( \mathbf{g}(f(x)) = (f(x) - v_1) \cdots (f(x) - v_r) \in \mathbb{K}(\mathbf{v})[x] \). Each \( f(x) - v_i \) is irreducible over \( \mathbb{K}(\mathbf{v}) \), and hence, also over \( \mathbb{K}(\mathbf{v}) \) (since \( \mathbb{K}(\mathbf{v})/\mathbb{K}(v_i) \) is purely transcendental). By the Fundamental Theorem of Symmetric Functions, \( k(\mathbf{v})/k(\mathbf{g}) \) is Galois, and its Galois group is the symmetric group \( S_r \). This group acts transitively on the irreducible factors \( f(x) - v_i \in \mathbb{K}(\mathbf{v})[x] \), which implies that their product \( \mathbf{g}(f(x)) \) is irreducible in \( \mathbb{K}(\mathbf{g})[x] \).

We verify now that (6.2) indeed enumerates all the irreducible factors of \( \text{disc}(\mathbf{g} \circ f) \) (which also implies the separability of \( \mathbf{g} \circ f \)). Write \( f'(x) = (x - \alpha_1) \cdots (x - \alpha_{n-1}) \in \mathbb{K}[x] \). It follows from [Odo85, Lemma 8.1 (i)] that \( \text{disc} \mathbf{g} \) is irreducible in \( \mathbb{K}[\mathbf{g}] \), and that

\[
\text{disc}(\mathbf{g} \circ f) = (\text{disc} \mathbf{g})^r \prod_{i=1}^r \text{disc}(f(x) - v_i) \in \mathbb{K}[\mathbf{v}].
\]

The \( r \)-term product above lies in \( \mathbb{K}[\mathbf{g}] \), indeed:

\[
\prod_{i=1}^r \text{disc}(f(x) - v_i) = \prod_{i=1}^r \prod_{j=1}^{n-1} (f(\alpha_j) - v_i) = \prod_{j=1}^{n-1} \mathbf{g}(f(\alpha_j)) \in \mathbb{K}[\mathbf{g}].
\]

Each \( \mathbf{g}(f(\alpha_j)) \in \mathbb{K}[\mathbf{g}] \), being linear in \( g_0, \ldots, g_{r-1} \), is irreducible in \( \mathbb{K}[\mathbf{g}] \), so we are done.

6.3. The curve \( C_f/k \) and group \( G_f \). Let \( K_f/k(u) \) denote a splitting field for \( f(x) - u \in k(u)[x] \), so that we have a factorization \( f(x) - u = (x - t_1) \cdots (x - t_n) \in K_f[x] \) in which the roots are pairwise distinct (by Lemma 6.1). The monodromy group of \( f \) is the Galois group

\[
G_f := \text{Gal}(f(x) - u/k(u)) = \text{Gal}(K_f/k(u)).
\]
Writing $R_f$ for the integral closure of $k[u]$ in $K_f$, the $G_f$-action on $K_f$ restricts to $R_f$, and $k[u]$ is the ring of invariants $(R_f)^{G_f}$. The Galois cover associated to $f$ is the finite $k$-morphism

$$\phi_f : C_f := \text{Spec } R_f \longrightarrow \mathbb{A}_k^1(u)$$

(6.5)
corresponding to the inclusion $k[u] \subset R_f$. It is the quotient by the (right) action of $G_f$ on $C_f/k$. Note that $C_f/k$ is geometrically integral if and only if $k$ is algebraically closed in $K_f$.

### 6.6. Constructing $\mathbb{K}_f/\mathbb{K}$

Identify the $k$-algebra $k[u]^\otimes r$ with the polynomial algebra $k[u] = k[u_1, \ldots, u_r]$ (from 4.4) by writing $u_i$ for the $i$-th simple tensor $1 \otimes \cdots \otimes u \otimes \cdots \otimes 1 \in k[u]^\otimes r$. By taking the $r$-fold tensor product (over $k$) of the inclusion $k[u] \hookrightarrow R_f$, we get an inclusion $k[u] \hookrightarrow R_f^\otimes r$. For each $i = 1, \ldots, r$ and $j = 1, \ldots, n$, let $t_{i,j} \in R_f^\otimes r$ denote the $i$-th simple tensor $1 \otimes \cdots \otimes t_{j} \otimes \cdots \otimes 1$ (where the $t_j$ is in the $i$-the place), so that $t_{i,1}, \ldots, t_{i,n}$ are the roots of $f(x) - u_i \in k[u][x]$. By construction, we have the factorization

$$\mathfrak{m}(f(x)) = \prod_{i=1}^{r} (f(x) - u_i) = \prod_{i=1}^{r} \prod_{j=1}^{n} (x - t_{i,j}) \in R_f^\otimes r[x].$$

(6.7)
The action of each monodromy group

$$G_{i,f} := \text{Gal}(f(x) - u_i/k(u_i)). \quad i = 1, \ldots, r$$

extends naturally to an action on $R_f^\otimes r$ in which $G_{i,f}$ fixes $t_{e,j}$ for every $e \neq i$. These together give an action of $G_f = \prod_{i=1}^{r} G_{i,f}$ on $R_f^\otimes r$ with ring of invariants $k[u]$. The cover of $k$-schemes $\phi_f^* : C_f \longrightarrow \mathbb{A}_k^r(u)$ is the quotient by the associated (right) action of $G_f$ on $C_f$. If $k$ is algebraically closed in $K_f$ then $C_f$ is a $k$-variety with function field $K_f^\otimes r$. So, the extension of function fields

$$\mathbb{K} = k(u) \hookrightarrow k(C_f) = K_f^\otimes r$$

(6.8)

induced by $\phi_f^*$ is Galois and we have a natural group isomorphism $\text{Gal}(k(C_f)/\mathbb{K}) \cong G_f$. This group acts faithfully on the roots $t_{i,j}$ of $\mathfrak{m}(f(x))$ in $k(C_f)$, which implies the following.

#### Lemma 6.9

If $K_f/k$ is regular, then $k(C_f)$ is a splitting field for $\mathfrak{m}(f(x)) \in \mathbb{K}[x]$, and we have

$$\text{Gal}(\mathbb{K}_f/\mathbb{K}) = \prod_{i=1}^{r} G_{i,f} \cong G_f.$$

#### Example 6.10

If $f(x)$ is quadratic then the inclusion $k(u) \subset k(t)$ defined by $u := f(t)$ makes $k(t)$ into a splitting field for $f(x) - u \in k(u)[x]$. So, we have $C_f = \mathbb{A}_k^1(t)$, $K_f = k(t)$, and $G_f = \mathbb{Z}_2$. Since $k(t)/k$ is regular, Lemma 6.9 says that the extension $\mathbb{K} \hookrightarrow k(t) := k(t_1, \ldots, t_r)$ defined by $u_i := f(t_i), \quad i = 1, \ldots, r$, makes $k(t)$ into a splitting field for $\mathfrak{m}(f(x)) \in \mathbb{K}[x]$.

#### Proposition 6.11

$\mathbb{K}_f$ is a rational function field over $k$ if and only if $C_f/k$ is birationally isomorphic to $\mathbb{P}_k^1$ (equivalently, $K_f$ is a one-dimensional rational function field over $k$).

**Proof.** The “if” direction is obvious. For the converse, suppose that $k_f(C_f)$ is a rational function field over $k$, or equivalently, that $C_f/k$ is $k$-birational to $\mathbb{P}_k^r$; this implies in particular that $K_f/k$ is regular. We can find inside $C_f$ an integral rational curve $U/k$ which possesses a $k$-point $P \in U(k)$. For some $i = 1, \ldots, r$, the $i$-th projection $\pi_i : C_f \longrightarrow C_f$ restricts to a non-constant $k$-morphism $\pi_i : U \longrightarrow C_f$. Then, $C_f/k$ is of genus 0 and has the point $\pi_i(P) \in C_f(k)$, which implies that $C_f$ is $k$-isomorphic to $\mathbb{P}_k^1$. \qed
Remark 6.12. The proof above implies in fact that $K_f$ is contained in a $2d$-dimensional rational function field over $k$ if and only if $C_f/k$ is birational to $P^1_k$.

6.13. Recall from 4.4 that $K$ denotes the field $k(h)$, and $M$ the field $k(m) = K(q)$. Consider now the chain of field extensions

$$k \hookrightarrow K \hookrightarrow M \hookrightarrow \mathbb{K} \hookrightarrow \mathbb{K}_f,$$

in which the first two extensions are each purely transcendental of degree $d + 1$ and the last two are finite. The curve $\mathbb{X}_f$ (and all its variants which we consider) will be defined over $K$, and they will be equipped with $\mathbb{K}_f$-points that are transcendental points (cf. 2.13). The next lemma furnishes (via Lemma 2.14) the key assumption (a2) of Lemma 6.12, which is used in the proof of Theorem 13.1 to determine the subgroups (of the respective Mordell–Weil groups) generated by these $\mathbb{K}_f$-points.

Lemma 6.15. If $k$ is algebraically closed and char $k = 0$, then $K$ is algebraically closed in $\mathbb{K}_f$.

Proof. Suppose for a contradiction that there exists a finite extension $F/K$ which is contained in $\mathbb{K}_f$. Let $S$ denote the integral closure of $k[h]$ in $F$, and let $\delta \in k[h]$ denote the discriminant of the $k[h]$-module $S$. Since char $k = 0$, there are no non-trivial connected étale covers of $A^{d+1}_k(h)$, so $\delta$ is not a unit in $k[h]$. The coordinate ring $R^{\text{or}}_f$ of $C_f$ is integrally closed in its fraction field $\mathbb{K}_f$, so $S$ is a subring of $R^{\text{or}}_f$. So, we have inclusions $k[m] = k[h][q] \hookrightarrow S[q] \hookrightarrow R^{\text{or}}_f$ which correspond to finite $k$-morphisms

$$C_f \hookrightarrow \text{Spec } S[q] \hookrightarrow A_k^{\text{or}}(m).$$

The branch locus $B'$ of the second morphism is cut out by $\delta \in k[m]$ (since it is obtained from the inclusion $k[h] \hookrightarrow S$ by tensoring with the polynomial ring $k[q]$). On the other hand, the branch locus $B$ of $C_f \hookrightarrow A_k^{\text{or}}(m)$ is cut out by $\text{disc}(m \circ f) \in k[m]$. Since $B' \subset B$, $\delta$ must divide $\text{disc}(m \circ f)$ in $k[m]$. But Lemma 6.1 says that the irreducible factors of $\text{disc}(m \circ f)$ in $k[m]$ (up to scaling by constants in $k^\times$) are $\text{disc }m = \text{disc}(q(x)^2 - h(x))$, and the elements of the form $\pm (f'(\alpha)) = q(f'(\alpha))^2 - h(\alpha)$, where $\alpha \in k$ is a root of $f'(x)$. None of these can equal $\delta$, since they do not lie in the subring $k[h] \subset k[m]$, so we have obtained a contradiction.

Remark 6.16. The proof above makes critical use of the fact that char $k = 0$ (namely, we make use of the fact that $A^{d+1}_k(h)$ does not admit any non-trivial connected étale covers in characteristic zero). We fully expect, nevertheless, that the statement of Lemma 6.15 continues to hold even if char $k > 0$. For example, if $f(x) = x^n$ then we can modify the argument as follows. We have in this situation $R^{\text{or}}_f := k[t] = k[t_1, \ldots, t_r]$, with the inclusion $k[u] \hookrightarrow k[t]$ defined by $u = t^n$. Then, the cover $C^f_\text{or} = \text{Spec } k[t] \to \text{Spec } k[m]$ is totally ramified at the origin $P = (0, \ldots, 0)$. This implies that any finite cover of $\text{Spec } S \to \text{Spec } k[h]$ arising as in the proof above must be ramified, and the rest of the proof carries through.

7. Polynomials having cyclic and dihedral monodromy groups

From now, until the end of the article, $k$ denotes a field of characteristic zero.

7.1. Proposition 6.11 invites consideration of the following problem: Produce polynomials $f(x) \in k[x]$ for which $K_f$ is a one-variable rational function field $k(z)$. We take as our starting point the observation that the monodromy group of such a polynomial must be a finite subgroup of $\text{Aut}_k(k(z)) = \text{PGL}_2(k)$. 

The determination of the finite subgroups of $\text{PGL}_2(\overline{k})$, for $k$ of characteristic zero, is classical. Apart from the three sporadic groups $A_4$, $S_4$, and $A_5^2$, which we will not consider in this article, $\text{PGL}_2(\overline{k})$ contains the family of cyclic groups $\{Z_n\}$ and the family of dihedral groups $\{D_n\}$.

For a given number field $k$, however, only finitely many of these occur in $\text{PGL}_2(k)$. Indeed, Beauville [Bea10] showed that $\text{PGL}_2(k)$ contains $Z_n$ if and only if $k$ contains $\lambda_n := \zeta_n^2 + \zeta_n^{-1}$; this is the source of the requirement in Theorem 1.3 that $k$ contain $\lambda_n, \lambda_{2n}$, or $\zeta_n$.

### 7.2. Cyclic monodromy

If $k$ contains $\zeta := \zeta_n$, then $\text{PGL}_2(k)$ contains $\sigma_n := [\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta_n \end{smallmatrix}]$. Identifying $\text{PGL}_2(k)$ with $\text{Aut}_k(k(u_n^{\text{cyc}}))$, this corresponds to the automorphism $u_n^{\text{cyc}} \mapsto \zeta u_n^{\text{cyc}}$, and the cover

$$f_n^{\text{cyc}} : A_k^1(u_n^{\text{cyc}}) \longrightarrow A_k^1(u), \quad u := (u_n^{\text{cyc}})^n,$$

is a quotient by $\langle \sigma_n \rangle$. The inclusion $k(u) \hookrightarrow k(u_n^{\text{cyc}})$ yields the factorization

$$x^n - u = \prod_{j=1}^n (x - \sigma_j(u_n^{\text{cyc}})) = \prod_{j=1}^n (x - \zeta^j u_n^{\text{cyc}}) \in k(u_n^{\text{cyc}})[x].$$

So, if $k$ contains $\zeta_n$ and $f(x) := x^n$, then $C_f = A_k^1(u_n^{\text{cyc}})$, $K_f = k(u_n^{\text{cyc}})$ and $G_f = \langle \sigma_n \rangle \cong Z_n$.

### 7.4. Dihedral monodromy with $\zeta_n$

Consider the element $\delta := [\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}] \in \text{PGL}_2(k)$. Identifying $\text{PGL}_2(k)$ with $\text{Aut}_k(k(u_n^{\text{dih}}))$, $\delta$ corresponds to the involution $u_n^{\text{dih}} \mapsto (u_n^{\text{dih}})^{-1}$. If $k$ contains $\zeta := \zeta_n$, we have again the automorphism $\sigma_n : u_n^{\text{dih}} \mapsto \zeta u_n^{\text{dih}}$, which together with $\delta$ generates a copy of $D_n$ inside $\text{Aut}_k(k(u_n^{\text{dih}}))$. To construct a quotient by this group, define

$$\text{Tr}(x) := x + x^{-1}, \quad f_n^{\text{dih}}(x) := x^n + x^{-n}.$$

Observe that $f_n^{\text{dih}}(x) \in k[x, x^{-1}]$ is invariant under the automorphism $x \mapsto x^{-1}$, whose ring of invariants is $k[\text{Tr}(x)]$. So, there exists some $f_n^{\text{re}}(x) \in k[x]$ which satisfies the identity

$$f_n^{\text{re}}(\text{Tr}(x)) = f_n^{\text{dih}}(x) = \text{Tr}(x^n) \in k[x, x^{-1}].$$

The rational function $f_n^{\text{dih}}$ has exactly two poles, each of order $n$, at the points $0$ and $\infty$. So, if we put $u_n^{\text{re}} := \text{Tr}(u_n^{\text{dih}})$ and $u_1^{\text{dih}} := (u_n^{\text{dih}})^n$, and write $G_{m, k}(u_n^{\text{dih}}) := \text{Spec} k[u_n^{\text{dih}}, (u_n^{\text{dih}})^{-1}] = \mathbf{P}_k^1(u_n^{\text{dih}}) - \{0, \infty\}$, then we have a cover

$$f_n^{\text{dih}} : G_{m, k}(u_n^{\text{dih}}) \longrightarrow A_k^1(u), \quad u := f_n^{\text{dih}}(u_n^{\text{dih}}) = f_n^{\text{re}}(u_n^{\text{re}}) = \text{Tr}(u_1^{\text{dih}}),$$

which is a quotient by $\langle \sigma_n, \delta \rangle \cong D_n$. Applying $\sigma_n^j$ to (7.5) has the effect of replacing $x$ with $\zeta^j x$, and it follows that (7.6) gives rise to the factorization

$$f_n^{\text{re}}(x) - u = \prod_{j=1}^n \left( x - \sigma_j^j(u_n^{\text{re}}) \right) = \prod_{j=1}^n \left( x - \left( \zeta^j u_n^{\text{dih}} + (\zeta^j u_n^{\text{dih}})^{-1} \right) \right) \in k(u_n^{\text{dih}})[x].$$

So, for $n \geq 3$, if $\zeta_n \in k$ and $f := f_n^{\text{re}}$, then $C_f = G_{m, k}(u_n^{\text{dih}})$, $K_f = k(u_n^{\text{dih}})$ and $G_f = \langle \sigma_n^{\text{dih}}, \delta \rangle \cong D_n$. Note that if $n = 1$ or $2$ then $k(u_n^{\text{re}})/k(u)$ is a quadratic extension of $k(u_n^{\text{re}})$, which is the splitting field of $f_n^{\text{re}}(x) - u$; see Example 6.10).

---

2Here, $A_n$ denotes the alternating group on $n$ letters.

3Here, $D_n$ denotes the dihedral group of order $2n$ which admits the presentation $D_n = \langle \delta, \sigma \mid \sigma^n, \delta^2, (\sigma \delta)^2 \rangle$. In particular, $D_1 \cong Z_2$ and $D_2 \cong V_4$ are both abelian groups.
7.8. Descent. In general, if $T/k$ is a commutative group scheme with a point $P \in T(k)$ of order $n$, then the translation-by-$P$ map $T \xrightarrow{\sim} T$ induces an order $n$ automorphism $\sigma \in \text{Aut}_k(k(T))$. This generates a dihedral group of order $2n$ with the involution $\delta \in \text{Aut}_k(k(T))$ corresponding to the inversion homomorphism $T \xrightarrow{\sim} T$. The construction in 7.4 is the special case when $T = \mathbb{G}_{m,k}$, so the requirement that $k$ contain $\zeta_n$ boils down to the fact that the $n$-th division field of $\mathbb{G}_{m,k}$ (i.e. the extension of $k$ generated by its points of order $n$) is $k(\zeta_n)$.

In the next subsection, we construct the splitting field for $f_n^0(x) - u$ with the more relaxed assumption $\lambda_n \in k^\times$. The basic idea is to replace the $\mathbb{G}_{m,k}$ with an algebraic torus $T_n/k$ whose $n$-th division field is $k(\lambda_n) = k$.

7.9. Dihedral monodromy with $\lambda_n$. Fix $n \geq 3$, and put $\lambda := \lambda_n$ and $\zeta := \zeta_n$. For simplicity, let $k$ be the real cyclotomic field $\mathbb{Q}(\lambda)$. The assumption $n \geq 3$ is equivalent to saying that $\ell := k(\zeta)$ is a quadratic extension of $k$. Let $\tau \in \text{Gal}(\ell/k)$ denote complex conjugation, and let $N_{\ell/k} : \ell^\times \rightarrow k^\times$ denote the usual norm homomorphism defined by $N_{\ell/k}(\alpha) := \alpha \tau(\alpha)$. Define

$$\overline{\omega}_n := s - \zeta \in \ell[s,t].$$

The norm-torus associated to $\ell/k$ is the affine plane curve

$$T_n/k : N_{\ell/k}(\overline{\omega}_n) = s^2 - \lambda st + t^2 = 1. \quad (7.10)$$

It is a one-dimensional algebraic $k$-torus (i.e. a $k$-group scheme which becomes isomorphic to $\mathbb{G}_{m,k}$ upon base-change to $\bar{k}$). We have a natural group isomorphism

$$T_n(k) \xrightarrow{\sim} N_{\ell/k}^1 := \{ \alpha \in \ell^\times \mid N_{\ell/k}(\alpha) = 1 \},$$

$$(s_0, t_0) \mapsto s_0 - \zeta t_0.$$  

The product of two $k$-points $\alpha$ and $\beta$ is the point $(s_0, t_0) \in T_n(k)$ determined by the identity $\alpha \beta = s_0 - \zeta t_0 \in N_{\ell/k}^1$. In particular, $(0, -1) \in T_n(k)$ corresponds to $\zeta \in N_{\ell/k}^1$, so we have $\zeta(s_0 - \zeta t_0) = t_0 - \zeta(\lambda t_0 - s_0)$. So, the multiplication-by-$\zeta$ map on $T_n$ induces the order $n$ automorphism $\sigma \in \text{Aut}_k(k(T_n))$ defined by

$$\overline{\omega}_n \sigma(s) = t \quad \text{and} \quad \overline{\omega}_n \sigma(t) = \lambda t - s. \quad (7.11)$$

By construction, the powers of $\overline{\omega}_n$ satisfy

$$\overline{\omega}_n^j(\overline{\omega}_n) = \zeta^j \overline{\omega}_n \in \ell(T_n), \quad \text{for} \ j = 1, \ldots, n. \quad (7.12)$$

Since $N_{\ell/k}(\overline{\omega}_n) = \overline{\omega}_n (s - \zeta^{-1} t) = 1 \in \ell(T_n)$, we have

$$\overline{\omega}_n^{-1} = s - \zeta^{-1} t = \tau(\overline{\omega}_n) \in \ell(T_n),$$

and it follows that $\text{Tr}(\overline{\omega}_n) = \text{Tr}_{\ell/k}(\overline{\omega}_n)$ is an element in $k(T_n)$. We put

$$\overline{\omega}_n^\ell := \text{Tr}(\overline{\omega}_n) = 2s - \lambda t \in k(T_n),$$

so that, for $j = 1, \ldots, n$, we have the identity

$$\overline{\omega}_n^j(\overline{\omega}_n^\ell) = \text{Tr}(\zeta^j(\overline{\omega}_n^\ell)) = \text{Tr}(\zeta^j)s - \text{Tr}(\zeta^j + 1)t \in k(T_n).$$

Now, the functional equation (7.5) implies that $f_n^\ell(\overline{\omega}_n^\ell) = f_n^\text{dih}(\overline{\omega}_n) \in k(T_n)$. Similar to the situation in 7.4, each automorphism $\overline{\omega}_n^j$ fixes $f_n^\text{dih}(\overline{\omega}_n) \in k(T_n)$, so applying $\overline{\omega}_n^j$ to this relation, we find that the cover

$$f_n^\text{dih} : T_n \longrightarrow \mathbb{A}_k^1(u)$$

$$u := f_n^\ell(\overline{\omega}_n) = f_n^\text{dih}(\overline{\omega}_n) \quad (7.13)$$
yields the factorization
\[ f_n^{re}(x) - u = \prod_{j=1}^{n} (x - \overline{\sigma}_j^{n}(\overline{u}_n^{e})) = \prod_{j=1}^{n} \left( x - (\text{Tr}(\zeta^j)x - \text{Tr}(\zeta^{j+1})) \right) \in k(T_n)[x]. \] (7.14)

We conclude that for \( n \geq 3 \), if \( k \) contains \( \lambda_n \) and \( f = f_n^{re}(x) \), then \( C_f = T_n \) and \( K_f = k(T_n) \). We will later need the following more precise statement.

**Lemma 7.15.** Let \( n \geq 3 \), assume that \( k \) contains \( \lambda_n \), and put \( \ell = k(\zeta_n) \). Then,
\[ \phi : \ell(\overline{u}_n^{dh}) \longrightarrow \ell(T_n), \quad \overline{u}_n^{dh} \longmapsto \overline{u}_n^{dh} \] (7.16)
is an isomorphism of \( \ell(u) \)-algebras which sends \( \sigma_n^{j}(\overline{u}_n^{e}) \in \ell(\overline{u}_n^{dh}) \) to the element \( \overline{\sigma}_n^{j}(\overline{u}_n^{e}) \in \ell(T_n) \), for \( j = 1, \ldots, n \). Thus, \( \phi \) transforms the factorization (7.14) into the factorization (7.7).

**Proof.** We have \( \phi((\overline{u}_n^{dh})^{-1}) = (\overline{u}_n^{dh})^{-1} = s - \zeta^{-1}t \in \ell(T_n) \). Using this, one checks that the map
\[ s \longmapsto \frac{\zeta^{-1}u_n^{dh} - \zeta(\overline{u}_n^{dh})^{-1}}{\zeta - \zeta^{-1}}, \quad t \longmapsto \frac{(\overline{u}_n^{dh})^{-1} - u_n^{dh}}{\zeta - \zeta^{-1}}. \]
defines the inverse \( \phi^{-1} : \ell(T_n) \longrightarrow \ell(\overline{u}_n^{dh}) \). That \( \phi \) is an isomorphism of \( \ell(u) \)-algebras follows because \( \phi(u) = \phi(f_n^{dh}(u_n^{dh})) = f_n^{dh}(\overline{u}_n^{dh}) = u \in \ell(T_n) \). The \( Z_n \)-actions on both fields are compatible with \( \phi \) in the sense that \( \phi(\sigma_n(u_n^{dh})) = \zeta_n\phi(u_n^{dh}) = \zeta(\overline{u}_n^{dh}) = \overline{\sigma}_n(\overline{u}_n^{dh}) \). Thus, \( \phi \) transforms each element \( \sigma_n^{j}(\overline{u}_n^{e}) = \text{Tr}(\zeta^j\overline{u}_n^{dh}) \) into the corresponding element \( \overline{\sigma}_n^{j}(\overline{u}_n^{e}) = \text{Tr}(\zeta^j(\overline{u}_n^{dh})) \). \( \square \)

**Example 7.17.** Let us illustrate the factorization (7.14) in the cases \( n = 3, 4 \) and 6 (namely, the cases used to obtain Corollary 1.6). Since \( \lambda_3 = -1, \lambda_4 = 0 \), and \( \lambda_6 = 1 \), we may work over \( k := \mathbb{Q} \). Then, the polynomials \( f_n^{re}(x) \) and the associated tori \( T_n/k \) are given by
\[ f_3^{re}(x) = x^3 - 3x, \quad T_3/k : s^2 + st + t^2 = 1, \]
\[ f_4^{re}(x) = x^4 - 4x^2 + 2, \quad T_4/k : s^2 + t^2 = 1, \]
\[ f_6^{re}(x) = x^6 - 6x^4 + 9x^2 - 2, \quad T_6/k : s^2 - st + t^2 = 1. \]

Defining the inclusions \( \mathbb{Q}(u) \hookrightarrow \mathbb{Q}(T_n) \) as in (7.13), the factorizations in (7.14) become:
\[ f_3^{re}(x) - u = (x + s + t)(x - s + 2t)(x - t + 2s), \]
\[ f_4^{re}(x) - u = (x - 2s)(x + 2s)(x - 2t)(x + 2t), \]
\[ f_6^{re}(x) - u = (x + s + t)(x - s - t)(x - s + 2t)(x + s - 2t)(x - t + 2s)(x + t - 2s). \]

**Remark 7.18.** We can construct a birational map between \( \mathbb{P}_k^1(z) \) and \( T_n \) by stereographic projection from the point \( (0, 1) \in T_n \). That is, we take \( z \) to be the slope of a line passing through \( (0, 1) \) and the generic point \( (s, t) \in T_n \), so that \( z = (t - 1)/s \in k(T_n) \). Replacing \( t \) with \( sz + 1 \) in the equation defining \( T_n \) and solving for \( s \) and \( t \) in terms of \( z \), we obtain
\[ s = \frac{\lambda - 2z}{z^2 - \lambda z + 1}, \quad t = \frac{1 - z^2}{z^2 - \lambda z + 1}, \]
so \( k(T_n) = k(z) \). One can check that \( \overline{\sigma}_n \in \text{Aut}_k(k(T_n)) \) corresponds to the order \( n \) automorphism \( z \longmapsto \frac{(\lambda + 1)z - 1}{z + 1} \in \text{Aut}_k(k(z)) \).
This is in fact the automorphism mentioned by Beauville in [Bea10] to conclude that $\mathbf{PGL}_2(k)$ contains $Z_n$ if $\lambda_n \in k$. Finally, we note that

$$\mathbf{PGL}_2^n = s - \zeta t = \frac{\zeta z - 1}{z - \zeta} \in \ell(T_n) = \ell(z).$$

Thus, the automorphism $\theta := \left[ \begin{array}{cc} \xi^{-1} & -1 \\ 1 & -1 \end{array} \right] \in \mathbf{PGL}_2(\ell)$ changes the coordinate on $\mathbf{P}^1$ from $z$ to $u$, and $\overline{\sigma}_n := \left[ \begin{array}{cc} \lambda & 1 \\ 1 & 0 \end{array} \right]$ and $\sigma_n := \left[ \begin{array}{cc} \xi & 0 \\ 0 & 1 \end{array} \right]$ are conjugate to each other by $\theta$, i.e. we have $\sigma_n = \theta \circ \overline{\sigma}_n \circ \theta^{-1} \in \mathbf{PGL}_2(\ell)$. The reader can moreover verify that the involution $\delta := \left[ \begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array} \right]$ commutes with $\theta$, so we have $\langle \sigma_n, \delta \rangle = \theta \circ (\sigma_n, \delta)^{-1} \subset \mathbf{PGL}_2(\ell)$.

**Remark 7.19.** If $\text{char } k > 0$, then the entire discussion in 7.2, 7.4 and 7.9 holds verbatim so long as $\text{char } k$ does not divide $2n$.

8. The rational function fields $\mathbb{k}_n^\text{cyc}$, $\mathbb{k}_n^\text{dih}$, and $\mathbb{k}_n^\text{re}$.

**8.1. Conventions.** We assume for this section that $\text{char } k = 0$. In what follows, the phrase “for each $i$” means “for $i = 1, \ldots, r$”. If $t = t_1, \ldots, t_r$ and $s = s_1, \ldots, s_r$ are $r$-tuples of indeterminates and $q(x) \in k(x)$ is a rational function, then we write $t = q(s)$ to abbreviate the collection of identities $t_i = q(s_i)$, for each $i$. We use the notation from 4.4; in particular $r = 2d + 2$ for a fixed positive integer $d$, and $\mathbb{k}$ denotes the rational function field $k(u) = k(u_1, \ldots, u_r)$.

**8.2. The fields $\mathbb{k}_n^\text{cyc}$, $\mathbb{k}_n^\text{dih}$, and $\mathbb{k}_n^\text{re}$.** Let $n \in \mathbb{N}$. Let $u_n^\text{cyc}$ and $u_n^\text{dih}$ denote the tuples of indeterminates $u_1^\text{cyc}, \ldots, u_r^\text{cyc}$ and $u_1^\text{dih}, \ldots, u_r^\text{dih}$. Let $u_n^\text{re}$ denote the $r$-tuple $u_1^\text{re}, \ldots, u_r^\text{re}$ defined by

$$u_n^\text{re} := \text{Tr}(u_n^\text{dih}) = (u_n^\text{dih}) + (u_n^\text{dih})^{-1}$$

Next, if $n \geq 3$ and $k$ contains $\lambda_n$, let $s$ and $t$ denote the tuples $s_1, \ldots, s_r$ and $t_1, \ldots, t_r$, and put $\overline{u}_n^\text{dih} := s - \zeta_n t$, so that

$$T_n/k : \{s^2 - \lambda_n st + t^2 = 1\} \subset \mathbf{A}_k^{2r}(s, t)$$

can naturally be identified with the $r$-fold product of the torus $T_n/k$ from 7.9. Let $\overline{u}_n^\text{re}$ denote the $r$-tuple $\overline{u}_1^\text{re}, \ldots, \overline{u}_r^\text{re}$ defined by

$$\overline{u}_n^\text{re} := \text{Tr}(\overline{u}_n^\text{dih}) = 2s - \lambda_n t.$$

Now, define the following extensions of rational function fields, (the third extension is defined below only for $n \geq 3$ and $k$ containing $\lambda_n$; in 8.12, we complete the picture by defining also $\mathbb{k}_n^\text{cyc}$):

$$\mathbb{k} \hookrightarrow \mathbb{k}_n^\text{cyc} := k(u_n^\text{cyc}), \quad u := (u_n^\text{cyc})^n,$$

$$\mathbb{k} \hookrightarrow \mathbb{k}_n^\text{dih} := k(u_n^\text{dih}), \quad u := f_n^\text{re}(u_n^\text{re}) = f_n^\text{dih}(u_n^\text{dih}),$$

$$\mathbb{k} \hookrightarrow \mathbb{k}_n^\text{re} := k(T_n), \quad u := f_n^\text{re}(\overline{u}_n^\text{re}) = f_n^\text{dih}(\overline{u}_n^\text{dih}).$$

Note in particular that $u = u_1^\text{cyc} = u_1^\text{re}$, and hence, we have $\mathbb{k} = \mathbb{k}_1^\text{cyc} = k(u_1^\text{cyc})$.

**8.4. Automorphisms.** If $k$ contains $\zeta_n$ and $\mathbb{k}_n = k(u_n)$ denotes $\mathbb{k}_n^\text{cyc} = k(u_n^\text{cyc})$ or $\mathbb{k}_n^\text{dih} = k(u_n^\text{dih})$, then define for each $i$ the automorphism

$$\sigma_{i,n} : u_{e,n} \longmapsto \begin{cases} \zeta_n u_{e,n} & \text{if } e = i, \\ u_{e,n} & \text{if } e \neq i. \end{cases} \in \text{Aut}_k(\mathbb{k}_n).$$

(8.5)
For the field \( k_n^{\text{cyc}} \), define also for each \( i \) the automorphism
\[
\delta_{i,n} : u_{e,n} \mapsto \begin{cases} 
(u_{e,n}^{\text{dih}})^{-1} & \text{if } e = i, \\
 u_{e,n}^{\text{dih}} & \text{if } e \neq i. 
\end{cases} \quad (8.6)
\]
Finally, if \( n \geq 3 \) and \( k \) contains \( \lambda_n \), then define for each \( i \) the automorphism
\[
\sigma_{i,n} : u_{e,n}^{\text{dih}} \mapsto \begin{cases} 
\zeta_n u_{e,n}^{\text{dih}} & \text{if } e = i, \\
 u_{e,n}^{\text{dih}} & \text{if } e \neq i. 
\end{cases} \quad (8.7)
\]

**Proposition 8.8.** Let \( n \in \mathbb{N} \).

(a) If \( k \) contains \( \zeta_n \), then we have the factorizations
\[
\mathfrak{m}(x^n) = \prod_{i=1}^{r} (x^n - u_i) = \prod_{i=1}^{r} \prod_{j=1}^{n} (x - \sigma^j_{i,n} (u_{i,n}^{\text{cyc}})) \in k_n^{\text{cyc}}[x], \quad (8.9)
\]
\[
\mathfrak{m}(f_n^{\text{re}}(x)) = \prod_{i=1}^{r} \left( f_n^{\text{re}}(x) - u_i \right) = \prod_{i=1}^{r} \prod_{j=1}^{n} \left( x - \sigma^j_{i,n} (u_{i,n}^{\text{re}}) \right) \in k_n^{\text{dih}}[x]. \quad (8.10)
\]

(b) If \( n \geq 3 \) and \( k \) contains \( \lambda_n \), then we have the factorization
\[
\mathfrak{m}(f_n^{\text{re}}(x)) = \prod_{i=1}^{r} \left( f_n^{\text{re}}(x) - u_i \right) = \prod_{i=1}^{r} \prod_{j=1}^{n} \left( x - \sigma^j_{i,n} (u_{i,n}^{\text{re}}) \right) \in k_n^{\text{re}}[x]. \quad (8.11)
\]

If moreover \( k \) contains \( \zeta_n \), then the map
\[
\phi_n : k_n^{\text{dih}} \xrightarrow{\sim} k_n^{\text{re}}, \quad u_n^{\text{dih}} \mapsto u_n^{\text{re}}, \quad (8.11)
\]
is a \( k \)-algebra isomorphism which sends
\[
\sigma^j_{i,n} (u_{i,n}^{\text{re}}) \mapsto \sigma^j_{i,n} (u_{i,n}^{\text{re}}), \quad \text{for } i = 1, \ldots, r.
\]
So, (8.11) transforms the factorization (8.10) into the second line of (8.9).

(c) If \( k \) is algebraically closed, then \( K = k(h) \) is algebraically closed in \( k_n^{\text{cyc}} \) and \( k_n^{\text{dih}} \). Consequently, for any abelian variety \( J/K \) we have an equality of torsion subgroups
\[
\mathcal{J}(K)_{\text{tors}} = \mathcal{J}(k_n^{\text{cyc}})_{\text{tors}} = \mathcal{J}(k_n^{\text{dih}})_{\text{tors}}.
\]

**Proof.** As in 6.6, identify the three extensions (8.3) with the \( r \)-th tensor power of the extensions \( k(u) \hookrightarrow k(u_n^{\text{cyc}}) \) from 7.2, \( k(u) \hookrightarrow k(u_n^{\text{dih}}) \) from 7.4, and \( k(u) \hookrightarrow k(T_n) \) from 7.9, respectively. Lemma 6.9 then implies that these give splitting fields for the respective \( \mathfrak{m}(f_n(x)) \)'s, and the factorizations (8.9) and (8.10) hold by construction. The isomorphism (8.11) is simply the \( r \)-th tensor power (over \( k \)) of the isomorphism (7.16). For part (c), assume that \( k \) is algebraically closed. Then, the extension \( k_n^{\text{cyc}}/k \) is nothing but the extension \( k_f/k \) for \( f = f_n^{\text{cyc}} \), so Lemma 6.15 implies that \( K \) is algebraically closed in \( k_n^{\text{cyc}} \). Similarly, for \( n \geq 3 \), \( k_n^{\text{dih}}/k \) is the extension \( k_f/k \) for \( f = f_n^{\text{re}} \), and since \( k \subset k_n^{\text{dih}} \subset k_n^{\text{cyc}} \), Lemma 6.15 implies that \( K \) is algebraically closed in \( k_n^{\text{dih}} \) for all \( n \in \mathbb{N} \). The statement about the torsion subgroups then follows from Lemma 2.14. \( \square \)

**8.12. Directed systems.** Arrange the fields \( \{k_n^{\text{cyc}}\}_{n \in \mathbb{N}} \) and \( \{k_n^{\text{dih}}\}_{n \in \mathbb{N}} \) into directed systems by defining for all \( n \in \mathbb{N} \) and all \( m \) dividing \( n \) the inclusion
\[
k_m^{\text{cyc}} \hookrightarrow k_n^{\text{cyc}}, \quad u_m^{\text{cyc}} := (u_n^{\text{cyc}})^{n/m},
k_m^{\text{cyc}} \hookrightarrow k_n^{\text{dih}}, \quad u_m^{\text{dih}} := (u_n^{\text{dih}})^{n/m}, \quad (8.13)
\]
Using the functional equation \((7.5)\), one checks that the above inclusions give (for \(m\) dividing \(n\)):
\[
\mathbf{u}^\text{re}_m = f^\text{re}_{n/m}(\mathbf{u}^\text{re}_n) \in \mathbb{K}^\text{dih}.
\] (8.14)
We will have need later for the \(r\)-tuple \(\mathbf{u}^\text{im}_n := \mathbf{u}^\text{im}_{1,n}, \ldots, \mathbf{u}^\text{im}_{r,n}\) defined by
\[
\mathbf{u}^\text{im}_n := (\mathbf{u}^\text{dih}_n)^r - (\mathbf{u}^\text{dih}_n)^{-1} \in \mathbb{K}^\text{dih}.
\]
If \(f^\text{im}_n(x) \in \mathbb{Z}[x]\) is the polynomial determined by the identity
\[
f^\text{im}_n(\text{Tr}(x)) = \frac{x^n - x^{-n}}{x - x^{-1}} \in \mathbb{Z}[x, x^{-1}],
\] (8.15)
then the following identities hold for every \(m \mid n \in \mathbb{N}\):
\[
\mathbf{u}^\text{im}_m = (\mathbf{u}^\text{im}_n f^\text{im}_{n/m}(\mathbf{u}^\text{im}_n)).
\] (8.16)
Next, for \(n \geq 3\) and \(k\) containing \(\lambda_{2n}\), we embed \(\mathbb{K}^\text{re}_n\) in \(\mathbb{K}^\text{re}_{2n}\) by sending the tuples \(\mathbf{s}\) and \(\mathbf{t}\) in \(\mathbb{K}^\text{re}_n\) to the tuples \(\mathbf{s}'\) and \(\mathbf{t}'\) in \(\mathbb{K}^\text{re}_{2n}\), respectively, which give the identity
\[
(\mathbf{u}^\text{dih}_{2n})^2 = \mathbf{s}' - \zeta_n \mathbf{t}' \in \mathbb{K}^\text{re}_{2n}(\zeta_n).
\]
In this way, we identify \(\mathbb{K}^\text{re}_n\) with the subfield of \(\mathbb{K}^\text{re}_{2n}\) generated over \(k\) by these \(r\)-tuples \(\mathbf{s}'\) and \(\mathbf{t}'\). To complete the picture with the case \(n = 2\), we similarly define the \(r\)-tuple of elements \(\mathbf{u}^\text{dih}_2 := \mathbf{s}' - \zeta_2 \mathbf{t}' \in \mathbb{K}^\text{dih}_2\) by the identity \(\mathbf{u}^\text{dih}_2 := (\mathbf{u}^\text{dih}_2)^2 \in \mathbb{K}^\text{dih}_2\), and we put
\[
\mathbb{K}^\text{re}_2 := k(\mathbf{s}', \mathbf{t}') \subset \mathbb{K}^\text{re}_4.
\]
Defining an isomorphism \(\phi_2 : \mathbb{K}^\text{dih}_2 \xrightarrow{\sim} \mathbb{K}^\text{re}_2\) by \(\mathbf{u}^\text{dih}_2 \mapsto \mathbf{u}^\text{re}_2\), the upshot of defining these inclusions is that we obtain for all \(n \geq 2\) a commutative diagram
\[
\begin{array}{ccc}
\mathbb{K}^\text{dih}_{2n} & \xrightarrow{\phi_{2n}} & \mathbb{K}^\text{re}_{2n} \\
\uparrow & & \uparrow \\
\mathbb{K}^\text{re}_{2n} & \xrightarrow{\phi_{n}} & \mathbb{K}^\text{re}_n,
\end{array}
\]
which in turn gives for all \(n \geq 2\) (using the functional equation \((7.5)\)) the identity \(f^\text{re}_{2n}(\mathbf{u}^\text{re}_{2n}) = \mathbf{u}^\text{re}_{2n} \in \mathbb{K}^\text{re}_{2n}\), equivalently,
\[
(\mathbf{u}^\text{re}_{2n})^2 = \mathbf{u}^\text{re}_{2n} + 2 \in \mathbb{K}^\text{re}_{2n}.
\] (8.17)

**Remark 8.18.** Exactly as in **Remark 7.19**, if \(\text{char}\ k\) is positive (and distinct from 2), then essentially everything in this section continues to hold if we restrict our attention to \(n\) not divisible by \(\text{char}\ k\). A notable (possible) exception to this is the statement of Proposition 8.8 (c) for the field \(\mathbb{K}^\text{dih}_n\), since the latter statement relies on **Lemma 6.15**, which in turn uses that \(\text{char}\ k = 0\) (note: **Remark 6.16** for an alternative argument which works for the cyclic case).

### 9. Defining the Curves and Stating the Point and Rank Bounds

**9.1.** Recall the notation from 8.2. Following the convention in 8.1, we put
\[
\mathbf{v} := q(\mathbf{u}) \in \mathbb{K},
\] (9.2)
so that the identity \(\mathfrak{m}(x) = \mathbb{h}(x)^2 - \mathbf{v}(x)\) from **Lemma 4.1** yields \(\mathbf{v}^2 = \mathbb{h}(\mathbf{u}) \in \mathbb{K}\). Consider now the following table of data; below, \([nd] \in \{0, 1\}\) denotes the remainder of \(nd\) mod 2 (so that \(nd + [nd]\) is always even).
We explain the remaining data of the table in the next proposition.

**Proposition 9.5.**

respectively.

Using this fact and the genus-degree formula for hyperelliptic curves, we have expressed in the last and third-last column of Table 9.3 the integer $nd$ in terms of the genera $g_n^*$ and $\tilde{g}_n^*$ of these curves. We explain the remaining data of the table in the next proposition.

(a) The integers $b_n^*$ and $\tilde{b}_n^*$ denote the number of $K$-rational Weierstrass points of $X_n^*$ and $\tilde{X}_n^*$, respectively.

(b) The third column of Table 9.3 defines an $r$-tuple of points

\[
Q_n^* := Q_{1,n}^*, \ldots, Q_{r,n}^* \in X_n^*(K_n), \quad \text{if } \zeta_n \in k, \\
\tilde{Q}_n^* := \tilde{Q}_{1,n}^*, \ldots, \tilde{Q}_{r,n}^* \in \tilde{X}_n^*(K_{2n}), \quad \text{if } \zeta_{2n} \in k.
\]  

(9.6)

(c) If $n \geq 2$, then we have $r$-tuples of points

\[
P_n^re := (u_n^re, v) \in X_n^re(K_n), \quad \text{if } \lambda_n \in k, \\
\tilde{P}_n^re := (\tilde{u}_n^re, \tilde{v}_n^re) \in \tilde{X}_n^re(K_{2n}), \quad \text{if } \lambda_{2n} \in k.
\]  

(9.7)
Moreover, if \( k \) contains \( \zeta_n \) (resp. \( \zeta_{2n} \)), the isomorphism \( \kappa^{\text{dih}} \overset{\sim}{\to} \kappa^{\text{re}} \) (resp. \( \kappa^{\text{dih}}_{2n} \overset{\sim}{\to} \kappa^{\text{re}}_{2n} \)) from (8.11) induces bijections (of sets of points and \( r \)-tuples):

\[
\begin{align*}
\mathcal{X}^r_n(\kappa^{\text{dih}}) & \overset{\sim}{\to} \mathcal{X}^r_n(\kappa^{\text{re}}), & (u^r_n, v) & \overset{\text{def}}{=} P^r_n \mapsto Q^r_n = (u^r_n, v), \\
\mathcal{X}^r_n(\kappa^{\text{dih}}_{2n}) & \overset{\sim}{\to} \mathcal{X}^r_n(\kappa^{\text{re}}_{2n}), & (u^r_n, v u^r_{2n}) & \overset{\text{def}}{=} P^r_n \mapsto Q^r_n = (u^r_n, v u^r_{2n}).
\end{align*}
\]

**Proof.** Part (a) follows by verifying in each case that \( b^*_n \) (resp. \( \tilde{b}^*_n \)) equals the number of \( K \)-rational roots of the polynomial \( \hat{g}^*_n(x) \) (resp. \( \hat{g}^*_n(x) \)), plus one if \( \deg \hat{g}^*_n(x) \) (resp. \( \deg \tilde{g}^*_n(x) \)) is odd; we leave this to the reader.

We turn now to parts (b) and (c). By (8.3), we have the identities

\[ u = f^\text{cyc}_n(u^{\text{cyc}}_n) = f^\text{re}(u^r_n) = f^\text{dih}(u^\text{dih}_n). \]

Plugging these into \( \hat{h}(x) \) and using the fact that \( \hat{h}(u) = v^2 \) immediately yields

\[ v^2 = f^\text{cyc}_n(u^{\text{cyc}}_n) = f^\text{re}(u^r_n) = f^\text{dih}(u^\text{dih}_n), \tag{9.8} \]

which proves that the formulas for \( Q^\text{cyc}_n \), \( Q^\text{re}_n \), and \( Q^\text{dih}_n \) indeed define \( r \)-tuples of points in \( \mathcal{X}^r_n(\kappa^{\text{cyc}}_{2n}), \mathcal{X}^r_n(\kappa^{\text{re}}_{2n}), \mathcal{X}^r_n(\kappa^{\text{dih}}_{2n}), \) and \( \mathcal{X}^r_n(\kappa^{\text{dih}}_{2n}) \), respectively. Recalling from (8.16) the identity \( (u^r_n)^2 = (u^\text{dih}_n)^2 - 4 \), we have that

\[ (v u^r_n)^2 = f^\text{re}_n(u^r_n)((u^r_n)^2 - 4) = f^\text{dih}_n(u^\text{dih}_n), \]

which verifies that \( P^\text{im}_n := (u^r_n, v u^r_n) \) defines an \( r \)-tuple in \( \mathcal{X}^r_n(\kappa^{\text{dih}}_{2n}) \). With this, we have dealt with the first half of Table 9.3. The analogous statements for the second half of the table and the tuple \( P^\text{dih}_n \) then follow by combining the identities (9.8) with the following identities (see (8.16) and (8.17)):

\[ (u^r_{2n})^2 = u^r_n + 2, \quad (u^\text{dih}_{2n})^2 = u^\text{dih}_n + 2, \quad \text{and} \quad (u^\text{im}_{2n})^2 = u^\text{im}_n - 2 \]

This proves that the formulas in Table 9.3 and (9.7) define \( r \)-tuples of points in the respective curves, as claimed. The final claim in part (c) follows now from Proposition 8.8 together with the fact that the isomorphism \( \kappa^{\text{dih}}_{2n} \overset{\sim}{\to} \kappa^{\text{re}}_{2n} \) sends each \( u_{i,2n}^r \) to \( u_{i,2n}^\text{re} \) and each \( u_{i,n}^r = (u_{i,2n}^r)^2 - 2 \) to \( u_{i,n}^\text{re} = (u_{i,2n}^\text{re})^2 - 2 \) (see 8.12). \( \square \)

The automorphisms from 8.4 act naturally on these \( r \)-tuples. In the next lemma we count the total number of Galois conjugates arising from these actions (the proof is a straightforward verification which is left to the reader).

**Proposition 9.9.** Fix \( n \in \mathbb{N} \) and the label \( \bullet \). Let \( \kappa_n \) denote the corresponding rational function field in Table 9.3. Recall the automorphisms of \( \kappa_n \) defined in 8.4. Then:

(a) If \( \bullet \in \{ \text{cyc}, \text{re}, \text{im} \} \), and \( \zeta_n \in k \) (resp. \( \zeta_{2n} \in k \)), then the points

\[ \begin{align*}
\cdot^\text{cyc} \sigma^j_{i,n}(Q_{i,n}^\bullet) & \in \mathcal{X}^r_n(\kappa_n), & i = 1, \ldots, r, & j = 1, \ldots, n, & e = 0, 1, \\
\cdot^\text{re} \sigma^j_{i,2n}(Q_{i,2n}^\bullet) & \in \mathcal{X}^r_n(\kappa_{2n}), & i = 1, \ldots, r, & j = 1, \ldots, 2n,
\end{align*} \]

are pair-wise distinct and hence contribute \( 2rn \) points to the respective curves.

(b) The curves \( \mathcal{X}_{2n}^{\text{dih}}/K \) and \( \widetilde{\mathcal{X}}_{2n}^{\text{dih}}/K \) admit the extra involution \( \delta : (x, y) \mapsto (x^{-1}, y/(x^{\ell+1})) \) (where \( g \) denotes the genus \( g^{\text{dih}}_{2n} \) or \( g^{\text{dih}}_{\text{re}} \) of the curves, respectively), and the points

\[ \begin{align*}
\cdot^\text{cyc} \tau^\ell \sigma_{i,n}^j(Q_{i,n}) & \in \mathcal{X}^r_n(\kappa^{\text{dih}}_{2n}), & i = 1, \ldots, r, & j = 1, \ldots, n, & \ell = 0, 1, e = 0, 1, \\
\cdot^\text{re} \sigma_{i,2n}^j(Q_{i,2n}) & \in \mathcal{X}^r_n(\kappa^{\text{re}}_{2n}), & i = 1, \ldots, r, & j = 1, \ldots, 2n, & \ell = 0, 1,
\end{align*} \]

are pair-wise distinct and hence contribute \( 4rn \) points to the respective curves.
(c) If \( n \geq 3 \) and \( k \) contains \( \lambda_n \), then the points
\[
\ell^j \sigma^i_{1,n}(P_{i,n}) \in \mathbb{X}_n^{\text{re}}(k_n), \quad i = 1, \ldots, r, \ j = 1, \ldots, n, \ e = 0, 1,
\]
are distinct and contribute \( 2rn \) points to \( \mathbb{X}_n^{\text{re}} \). Similarly, if \( n \geq 2 \) and \( k \) contains \( \lambda_{2n} \), then the points
\[
\bar{\sigma}^j_{1,2n}(P_{i,n}) \in \bar{\mathbb{X}}_n^{\text{re}}(\bar{k}_{2n}), \quad i = 1, \ldots, r, \ j = 1, \ldots, 2n,
\]
are distinct and contribute \( 2rn \) points to \( \bar{\mathbb{X}}_n^{\text{re}} \).

9.10. Fix \( n \in \mathbb{N} \) and \( \bullet \in \{ \text{cyc, re, im, dih} \} \). Assume that \( \zeta \in k \), so that we may consider the tuple of points \( Q_n^\bullet \in \mathbb{X}_n^\bullet(\mathbb{K}_n) \). Viewing \( \mathbb{X}_n^\bullet(\mathbb{K}_n) \) as a module over the Galois group
\[
\mathbb{G}_n := \text{Gal}(\mathbb{K}_n/\mathbb{K}),
\]
we define the degree zero divisors \( 2Q_n^\bullet = D_\infty \) (cf. 2.3) and we define
\[
W_{i,n} := \text{span}_{\mathbb{Z}\mathbb{G}_n} \{ Q_{i,n} \}, \quad W_n^\bullet := W_{1,n}^\bullet \oplus \cdots \oplus W_{r,n}^\bullet \subset \text{Div}^0(\mathbb{X}_n^\bullet)_{k_n}.
\]
Similarly, if \( \zeta_{2n} \in k \) then we have the divisors \( \bar{Q}_{i,n} := 2\bar{Q}_{i,n} - D_\infty \) and we can define
\[
\bar{W}_{i,n} := \text{span}_{\mathbb{Z}\mathbb{G}_n} \{ \bar{Q}_{i,n} \}, \quad \bar{W}_n^\bullet := \bar{W}_{1,n}^\bullet \oplus \cdots \oplus \bar{W}_{r,n}^\bullet \subset \text{Div}^0(\bar{\mathbb{X}}_n^\bullet)_{\bar{k}_{2n}}.
\]
For each of these spaces \( W \), we denote by \([W]\) the image of \( W \) under the natural map from \( \text{Div}^0 \) to \( \text{Pic}^0 \) which sends a degree zero \( \mathbb{Q} \)-divisor \( E \) to its class \([E]\). Thus, the integers
\[
R_n^\bullet := \text{dim}_\mathbb{Q}[W_n^\bullet], \quad \bar{R}_n^\bullet := \text{dim}_\mathbb{Q}[\bar{W}_n^\bullet]
\]
serve as lower bounds for the rank of \( \mathbb{X}_n^\bullet/\mathbb{K}_n \) (resp. \( \bar{\mathbb{X}}_n^\bullet/\bar{k}_{2n} \)).

Similarly, for \( \bullet \in \{ \text{cyc, re, im} \} \), we define the integers
\[
N_n^\bullet := 2rn + b_n^\bullet, \quad \bar{N}_n^\bullet := 2rn + \bar{b}_n^\bullet,
\]
and for the dihedral curves, we define
\[
N_n^{\text{dih}} := 4rn + b_n^{\text{dih}}, \quad \bar{N}_n^{\text{dih}} := 4rn + \bar{b}_n^{\text{dih}}.
\]

Lemma 9.14. For \( n \in \mathbb{N} \) and each \( \bullet \):

(a) We have the lower bounds
\[
\#\mathbb{X}_n^\bullet(\mathbb{K}_n) \geq N_n^\bullet \quad \text{and} \quad \text{rk} \ \mathbb{X}_n^\bullet/\mathbb{K}_n \geq R_n^\bullet, \quad \text{if} \ \zeta \in k,
\]
\[
\#\bar{\mathbb{X}}_n^\bullet(\bar{k}_{2n}) \geq \bar{N}_n^\bullet \quad \text{and} \quad \text{rk} \ \bar{\mathbb{X}}_n^\bullet/\bar{k}_{2n} \geq \bar{R}_n^\bullet, \quad \text{if} \ \zeta_{2n} \in k.
\]

(b) If \( n \geq 3 \), then we have the lower bounds
\[
\#\mathbb{X}_n^{\text{re}}(k_n) \geq N_n^\bullet \quad \text{and} \quad \text{rk} \ \mathbb{X}_n^{\text{re}}/k_n \geq R_n^\bullet, \quad \text{if} \ \lambda_n \in k,
\]
\[
\#\bar{\mathbb{X}}_n^{\text{re}}(\bar{k}_{2n}) \geq \bar{N}_n^\bullet \quad \text{and} \quad \text{rk} \ \bar{\mathbb{X}}_n^{\text{re}}/\bar{k}_{2n} \geq \bar{R}_n^\bullet, \quad \text{if} \ \lambda_{2n} \in k.
\]

Proof. For (a), the lower bound on the number of points follows by counting the points coming from Proposition 9.9 together with the \( b_n^\bullet \) (or \( \bar{b}_n^\bullet \)) Weierstrass points, and the statement about the rank is obvious. Part (b) is an immediate consequence of Proposition 9.5 (c) and the fact that the isomorphism \( \phi : \mathbb{K}^{\text{dih}}_n \overset{\sim}{\longrightarrow} \mathbb{K}^{\text{re}}_n \) from Proposition 8.8 induces a bijection from the Gal(\( \mathbb{K}^{\text{dih}}_n/\mathbb{K} \))-conjugates of \( Q_n^{\text{re}} \in \mathbb{X}_n^{\text{re}}(\mathbb{K}^{\text{dih}}_n) \) to the Gal(\( \mathbb{K}^{\text{re}}_n/\mathbb{K} \))-conjugates of \( P_n^{\text{re}} \). The proof for \( \bar{\mathbb{X}}_n^{\text{re}} \) is similar. □

Now, the bulk of the remainder of the paper is devoted to proving the following.

Theorem 9.17 (Proved in 13.6). The integers \( R_n^\bullet \) and \( \bar{R}_n^\bullet \) satisfy the values in the following table.
9.19. Proof strategy. We will proceed in three steps:

(i) First, we show in Lemma 10.7 that Theorem 9.17 holds in full generality if it holds for the integers $R_n^{cyc}$, $R_n^{re}$, and $R_n^{im}$. This follows by exploiting the fact that the curves $X_n^{*}/K$ and $\tilde{X}_n^{*}/K$ are related by various covers which induce various isogeny relations between the respective Jacobians.

(ii) Next, in Proposition 12.2 we reduce the task of determining the integers $R_n^{cyc}$, $R_n^{re}$ and $R_n^{im}$ to determining, in each case (and for all $n \in \mathbb{N}$), the dimension of a certain distinguished subspace $[V_n^{*}] \subset [W_n^{*}]$. This again follows by exploiting the fact that each family $\{X_n^{*}\}_{n \in \mathbb{N}}$ forms an inverse system with very nice properties (see Section 11).

(iii) Finally, in Theorem 13.1 we apply the rank-bounding tools from Section 2 to determine the dimension of each space $[V_n^{*}]$, and we complete the proof of Theorem 9.17.

We conclude this section by showing how Theorem 1.3 follows from Theorem 9.17, using the fact (proved in Proposition 14.1) that any positive genus curve in the real, imaginary, and dihedral families is non-isotrivial over its field of definition $K$.

9.20. Proof of Theorem 1.3. There are five cases to consider, depending on the value of $dn$ (in terms of $g$); we use below the fact that $2rn = 4dn + 4n$, and the fact that for odd $n$ we have $Q(\lambda_n) = Q(\lambda_{2n})$ and $Q(\zeta_n) = Q(\zeta_{2n})$.

- $2g + 2$: If $nd$ is even then $nd = 2g_n^{re} + 2$. If $\lambda_n \in k$ then Theorem 9.17 gives
  $$\#X_n^{re}(k_n^{re}) \geq 2rn + b_n^{re} = 8g_n^{re} + 4n + 8.$$

- $2g + 1$: If $nd$ is odd then $nd = 2g_n^{re} + 1$. If $\lambda_n \in k$, then also $\lambda_{2n} \in k$, so Theorem 9.17 gives
  $$\#\tilde{X}_n^{re}(k_{2n}^{re}) \geq 2rn + b_n^{re} = 8g_n^{re} + 4n + 5.$$

- $2g$: If $nd$ is even then $nd = 2g_n^{im}$ and $b_n^{im} = 2$, which implies that $\tilde{J}_n^{im}$ has a $K$-rational point of order 2. If $\lambda_{2n} \in k$ then Theorem 9.17 gives
  $$\#\tilde{X}_n^{im}(k_{2n}^{im}) \geq 2rn + b_n^{im} = 8g_n^{im} + 4n + 2.$$

- $2g - 1$: If $nd$ is odd then $nd = 2g_n^{im} - 1$ and $b_n^{im} = 3$, so $J_n^{im}$ has three $K$-points of order 2 which generate the group $V_4$ inside $J_n^{im}(K)$. If $\zeta_n \in k$ then Theorem 9.17 gives
  $$\#X_n^{im}(k_n^{im}) \geq 2rn + b_n^{im} = 8g_n^{im} + 4n - 1.$$

- $g + 1$: If $nd$ is even then $nd = 8g_n^{dih} + 1$, so if $\zeta_n \in k$ then Theorem 9.17 gives
  $$\#\tilde{X}_n^{dih}(k_{2n}^{dih}) \geq 4rn + b_n^{dih} = 8g_n^{dih} + 8n + 8.$$

\[\begin{array}{|c|c|c|c|c|c|}
\hline
 & d = 1 & d = 2 & d \geq 3 \\
\hline
\bullet & R_n^{*} & \tilde{R}_n^{*} & R_n^{*} & \tilde{R}_n^{*} & R_n^{*} & \tilde{R}_n^{*} \\
\hline
\text{cyc} & 8g_n^{cyc} & 8g_n^{cyc} & 6g_n^{cyc} & 6\tilde{g}_n^{cyc} & \text{rn} - 1 & \text{rn} \\
\text{re} & 8g_n^{re} & 8g_n^{re} & 6g_n^{re} & 6\tilde{g}_n^{re} & \text{rn} - 1 & \text{rn} \\
\text{im} & 8g_n^{im} - 4 & 8g_n^{im} & 6g_n^{im} & 6\tilde{g}_n^{im} & \text{rn} & \text{rn} \\
\text{dih} & 8g_n^{dih} - 4 & 8g_n^{dih} & 6g_n^{dih} & 6\tilde{g}_n^{dih} & 2\text{rn} - 1 & 2\text{rn} \\
\hline
\end{array}\]
If \( nd \) is odd then \( nd = \frac{g_n}{2} + 1 \), and if \( \zeta_n \in k \), then also \( \zeta_{2n} \in k \); so, Theorem 9.17 gives
\[
\#\mathbb{X}_n^{\text{dih}}(K) \geq 4rn + \frac{g_n}{2} = 8g_n + 8n + 8.
\]
One checks, in each of the five cases above, that the rank bounds in Table 9.18 coincide with the corresponding bounds given in Theorem 1.3. In all cases considered, the points are defined over a rational function field over \( K \). The desired result now follows by specialization (more precisely, Corollary 3.5).

### 10. First reduction: partner curves

**Lemma 10.1.** Let \( X/K \) be a hyperelliptic curve which admits double covers

\[
\begin{array}{c}
\phi \\
\downarrow \\
Y
\end{array} \quad \begin{array}{c}
\tilde{\phi} \\
\downarrow \\
\tilde{Y}
\end{array}
\]

Let \( \tau \) and \( \tilde{\tau} \in \text{Aut}_K(X) \) be the involutions with quotients \( \phi \) and \( \tilde{\phi} \), respectively. Assume that \( \tilde{\tau} = \tau \tau \in \text{Aut}_K(X) \) (cf. 2.3). Then, the homomorphism
\[
(\phi_*, \tilde{\phi}_*) : J_X \longrightarrow J_Y \times J_{\tilde{Y}}
\]
is a \( K \)-isogeny, with dual isogeny defined by
\[
\phi^* + \tilde{\phi}^* : J_Y \times J_{\tilde{Y}} \longrightarrow J_X.
\]

Following Shioda [Shi98], we call the curves \( Y \) and \( \tilde{Y} \) above partner curves relative to \( X \).

**Proof.** The key point is that \( \tau P = -P \) for any geometric point \( P \in J_X(\overline{K}) \) (because if \( P \) is represented by a divisor class \([D]\), then \( P + \tau P = \pi^*[\pi_*D] = 0 \in J_X(\overline{K}) \)). So, we have \( \tau P = -\tau P \in J_X(\overline{K}) \), giving
\[
(\phi^* + \tilde{\phi}^*) \circ (\phi_*, \tilde{\phi}_*)(P) = \phi^* \phi_*(P) + \tilde{\phi}^* \tilde{\phi}_*(P) = (1 + \tau)P + (1 - \tau)P = 2P,
\]
as desired. \( \square \)

#### 10.2. Coordinates and double covers.

Let \( n \in \mathbb{N} \). We label the coordinates \((x, y)\) on each of the curves \( \mathbb{X}_n^* \) and \( \tilde{\mathbb{X}}_n^* \) from (9.4) as follows. For \( \bullet \in \{\text{cyc, re, dih}\} \), we write \((x_n^*, y_n^*)\) and \((\tilde{x}_n^*, \tilde{y}_n^*)\) for the coordinates on \( \mathbb{X}_n^* \) and \( \tilde{\mathbb{X}}_n^* \), respectively. On the other hand, we write \((x_n^{\text{re}}, y_n^{\text{im}})\) and \((\tilde{x}_n^{\text{re}}, \tilde{y}_n^{\text{im}})\) for the coordinates on \( \mathbb{X}_n^{\text{im}} \) and \( \tilde{\mathbb{X}}_n^{\text{im}} \), respectively. In the next table, we define various formulas relating the coordinates which define double covers between the respective curves; below, \( \text{Tr}_+(x) \) denotes the rational function \( x - x^{-1} \). We note also that \( f_2^{\text{re}}(x) = x^2 - 2 \in \mathbb{Z}[x] \).
The next proposition records the fact that for each pair of double covers in a row of Table 10.3, the two targets are partner curves relative to the source (cf. Lemma 10.1). We write $\mathbb{J}^\bullet_n/K$ and $\tilde{\mathbb{J}}^\bullet_n/K$ for the Jacobians of $\mathbb{X}^\bullet_n/K$ and $\tilde{\mathbb{X}}^\bullet_n/K$, respectively.

**Proposition 10.5.** For $n \in \mathbb{N}$, the following are $K$-isogenies:

\[
\begin{align*}
((\psi_n^{\text{re}})_\bullet, (\psi_n^{\text{im}})_\bullet) & : \mathbb{J}^\text{dih}_n \longrightarrow \mathbb{J}^\text{re}_n \times \mathbb{J}^\text{im}_n, \\
((\tilde{\psi}_n^{\text{re}})_\bullet, (\tilde{\psi}_n^{\text{im}})_\bullet) & : \mathbb{J}^\text{dih}_n \longrightarrow \tilde{\mathbb{J}}^\text{re}_n \times \tilde{\mathbb{J}}^\text{im}_n, \\
((\phi_n^\bullet)_\bullet, (\tilde{\phi}_n^\bullet)_\bullet) & : \mathbb{J}^\bullet_{2n} \longrightarrow \mathbb{J}^\bullet_{2n} \times \mathbb{J}^\bullet_{2n},
\end{align*}
\]

for $\bullet \in \{\text{cyc, re, im, dih}\}.$

**Proof.** For $\bullet = \text{re}$ and cyc, the double covers $\phi^\bullet_n$ and $\tilde{\phi}^\bullet_n$ are respectively quotients by the involutions

\[
\begin{align*}
\tau_n : (x_{2n}^\bullet, y_{2n}^\bullet) & \mapsto (-x_{2n}^\bullet, y_{2n}^\bullet), \\
\tilde{\tau}_n : (x_{2n}^\bullet, y_{2n}^\bullet) & \mapsto (-x_{2n}^\bullet, -y_{2n}^\bullet).
\end{align*}
\]
The covers \( \phi_n^{\text{im}} \) and \( \phi_n^{\text{re}} \), on the other hand, are respectively quotients by
\[
\tau_n : (x_{2n}^{\text{re}}, y_{2n}^{\text{im}}) \mapsto (-x_{2n}^{\text{re}}, -y_{2n}^{\text{im}}), \quad \tau_n : (x_{2n}^{\text{re}}, y_{2n}^{\text{im}}) \mapsto (-x_{2n}^{\text{re}}, y_{2n}^{\text{im}}),
\]
and \( \phi_n^{\text{im}} \) and \( \phi_n^{\text{re}} \) are respectively quotients by
\[
\tau_n : (x_{2n}^{\text{im}}, y_{2n}^{\text{re}}) \mapsto (-x_{2n}^{\text{im}}, -y_{2n}^{\text{re}}), \quad \tau_n : (x_{2n}^{\text{im}}, y_{2n}^{\text{re}}) \mapsto (-x_{2n}^{\text{im}}, y_{2n}^{\text{re}}).
\]
In all four of these cases, we have the relation ~
\[
\leq_{9.19}\text{.}
\]

Following the strategy in 9.19, we reduce the proof of Theorem 9.17 as follows.

\textbf{Lemma 10.7.} For all \( n \in \mathbb{N} \), we have \( R_n^{\text{dih}} = R_n^{\text{re}} + R_n^{\text{im}} \), and for all four values of \( \bullet \), we have \( \tilde{R}_n^\bullet = R^\bullet_{2n} - R^\bullet_n \). Consequently, if the values for \( R_n^{\text{re}} \), \( R_n^{\text{im}} \) and \( R_n^{\text{dih}} \) in Table 9.18 are correct for all \( n \in \mathbb{N} \), then Theorem 9.17 holds.

\textit{Proof.} First note that \( \psi_n^{\text{re}} \) and \( \psi_n^{\text{im}} \) map the r-tuple \( Q_n^{\text{dih}} \in \mathbb{X}_n^{\text{dih}}(K_n) \) to the r-tuples \( Q_n^{\text{re}} \in \mathbb{X}_n^{\text{re}}(K_n) \) and \( Q_n^{\text{im}} \in \mathbb{X}_n^{\text{im}}(K_n) \), respectively. Thus, they give rise to surjections \( \psi_n^{\text{re}} : W_n^{\text{dih}} \twoheadrightarrow W_n^{\text{re}} \) and \( \psi_n^{\text{im}} : W_n^{\text{dih}} \twoheadrightarrow W_n^{\text{im}} \). The first isogeny from (10.6) then induces an isomorphism of \( \mathbb{Q} \)-vector spaces
\[
((\psi_n^{\text{re}})^*, (\psi_n^{\text{im}})^*) : W_n^{\text{dih}} \cong W_n^{\text{re}} \oplus W_n^{\text{im}},
\]
which proves that \( R_n^{\text{dih}} = R_n^{\text{re}} + R_n^{\text{im}} \). An identical argument serves to show that for each \( \bullet \) the third isogeny from (10.6) induces an isomorphism of \( \mathbb{Q} \)-vector spaces
\[
((\phi_n^{\text{re}})^*, (\phi_n^{\text{im}})^*) : W_n^{\text{dih}} \cong W_n^{\text{re}} \oplus W_n^{\text{im}},
\]
which proves that \( \tilde{R}_n^\bullet = R^\bullet_{2n} - R^\bullet_n \). In particular, we recover \( \tilde{R}_n^{\text{dih}} \) as \( \tilde{R}_n^{\text{dih}} = (R_{2n}^{\text{re}} + R_{2n}^{\text{im}}) - (R_n^{\text{re}} + R_n^{\text{im}}) \). The desired result now follows by checking that these identities are satisfied by the values in Table 9.18; we leave this calculation to the reader. \( \square \)

11. \( \hat{Z} \)-systems and New Parts Decompositions

11.1. \( \hat{Z} \)-systems. View the set \( \mathbb{N} \) of positive integers as a poset via the “inverted” divisibility relation on \( \mathbb{N} \) in which \( n \leq m \) if and only if \( m \) divides \( n \) (denoted \( m \mid n \)). We write \( m \parallel n \) if \( m \mid n \) and \( m < n \). By a \( \hat{Z} \)-system (of nice curves) over \( K \), we mean an inverse system \(((\mathbb{X}_n/K)_{n \in \mathbb{N}}, (\phi_{n,m})_{m \mid n \in \mathbb{N}})\) (abbreviated by writing \((\mathbb{X}_n, \phi_{n,m})\)) of nice curves over \( K \) in which each morphism \( \phi_{n,m} : \mathbb{X}_n \to \mathbb{X}_m \) is a cover which of degree \( n/m \).
11.3. The new parts \( A_n/K \). Let \( (X_n, \phi_{n,m}) \) be a \( \hat{Z} \)-system of curves over \( K \), and for each \( n \in \mathbb{N} \), let \( J_n/K \) denote the Jacobian of \( X_n/K \). Then each \( \phi_{n,m} \) gives rise to two homomorphisms of abelian varieties over \( K \), namely

\[
(\phi_{n,m})_* : J_n \to J_m, \quad [D] \mapsto [(\phi_{n,m})_* D],
\]

\[
(\phi_{n,m})^* : J_m \to J_n, \quad [E] \mapsto [(\phi_{n,m})^* E].
\]

For each \( n \geq 2 \), we define the following abelian sub-variety of \( J_n/K \):

\[
A_n/K := \text{The identity component of } \bigcap_{m \mid n} \ker \left( J_n \xrightarrow{(\phi_{n,m})_*} J_m \right).
\] (11.4)

**Lemma 11.5.** Let \( d \) and \( m \) be positive integers, neither of which divides the other, and put \( \ell := \text{lcm}(d, m) \). Then, we have

\[
(\phi_{\ell,m})_* \circ (\phi_{\ell,d})^* = 0 \in \text{Hom}(A_d, J_m).
\]

**Proof.** Put \( h := \gcd(d, m) \). The desired result follows from the claim that

\[
(\phi_{\ell,m})_* (\phi_{\ell,d})^* = (\phi_{d,h})^* (\phi_{d,h})_* \in \text{Hom}(J_d, J_m).
\] (11.6)

Let \( B \subset X_h \) denote the set of branch points of \( \phi_{d,h} \circ \phi_{\ell,d} \). Put \( Y_h := X_h \setminus B \), and let \( Y_d, Y_m \), and \( Y_\ell \) denote the open subsets of \( X_d, X_m \), and \( X_\ell \) obtained by removing the pre-image of \( B \) under the respective morphism to \( X_h \). Any geometric point of \( J_d \) can be represented by the class of some divisor \( D \in \text{Div}^0(Y_d/K) \), so to prove (11.6), it suffices to show that

\[
(\phi_{\ell,m})_* (\phi_{\ell,d})^* = (\phi_{d,h})^* (\phi_{d,h})_* \in \text{Hom}(\text{Div} Y_d, \text{Div} Y_m).
\]

For this, it suffices to show that for any geometric point \( P \in Y_d(K) \), we have

\[
(\phi_{\ell,m})_* (\phi_{\ell,d})^*(P) = (\phi_{d,h})^* (\phi_{d,h})_* (P).
\]
This in turn would follow from the claim that the following diagram of affine curves is Cartesian:

\[
\begin{array}{ccc}
Y_\ell & \xrightarrow{\phi_{\ell,d}} & Y_d \\
| & & | \\
\phi_{d,h} & & \phi_{m,h}
\end{array}
\]

That is, we want to show that the natural induced morphism of \(Y_h\)-schemes

\[
Y_\ell \longrightarrow Y_d \times_{Y_h} Y_m
\]  

(11.7)
is an isomorphism. To see this, let \(L_i\) denote the function field of each \(Y_i\), and note that the restriction of (11.7) to the generic point of \(Y_h\) gives rise to a homomorphism of \(L_h\)-algebras

\[
L_d \otimes_{L_h} L_m \longrightarrow L_\ell.
\]  

This must be an isomorphism because the existence of a non-trivial kernel would imply the existence of an intermediate field \(L_h \subset L \subset L_d\) that admits an embedding (over \(L_h\)) into \(L_m\), which is impossible since the degrees \([L_d : L_h] = d/h\) and \([L_m : L_h] = m/h\) are co-prime. Thus, (11.7) is at least a birational isomorphism. Since the source and target are both finite étale of degree \(\ell/h = dm/h^2\) over \(Y_h\), (11.7) is also an isomorphism. This concludes the proof.  

To streamline notation, we put \(A_1/K := J_1/K\). The next lemma makes precise the notion that \(A_n\) is the “new part” of \(J_n\), with the “old part” being the abelian sub-variety generated by the images \((\phi_{n,m})^*J_m\), for \(m \parallel n\). We note that the previous lemma furnishes the commutativity of the diagram (11.11) below, which constitutes a crucial step in the proof.

**Lemma 11.8.** Let \(n \in \mathbb{N}\), and put \(B_n := \prod_{m \mid n} A_m\). Then, the homomorphism

\[
\Theta_n := \sum_{m \mid n} \phi_{n,m}^* \in \text{Hom}(B_n, J_n)
\]  

(11.9)
is a \(K\)-isogeny. Consequently, the genus \(g_n\) of \(X_n\) and dimension \(a_n\) of \(A_n\) satisfy the identities

\[
g_n = \sum_{m \mid n} a_m \quad \text{and} \quad a_n = \sum_{m \mid n} \mu(m)g_{n/m},
\]  

(11.10)

where \(\mu(\cdot)\) denotes the Möbius function.

We call the isogeny \(\Theta_n : B_n \longrightarrow J_n\) the new parts decomposition of \(J_n\).

**Proof.** The second identity in (11.10) follows by applying Möbius inversion to the first identity, which itself follows from the claim that \(\Theta_n\) is a \(K\)-isogeny, so we need only prove the latter. Recall that the isogeny category \(\text{Isog}_K\) is the abelian category in which the objects are abelian varieties over \(K\) and the hom-sets, for objects \(A, B \in \text{Isog}_K\), are the \(\mathbb{Q}\)-vector spaces \(\text{Hom}^0(A, B) = \text{Hom}(A, B) \otimes \mathbb{Q}\). The Poincaré Reducibility Theorem implies that \(\text{Isog}_K\) is a semi-simple category, i.e. that any \(J \in \text{Isog}_K\) admits a decomposition \(J \cong B_1^{e_1} \times \cdots \times B_r^{e_r}\), in which each \(B_i/K\) is simple. We note here that giving an isomorphism \(A \longrightarrow B\) in \(\text{Isog}_K\) is equivalent to giving a \(K\)-isogeny \(A \longrightarrow B\). So, in the present situation our goal is to show that \(\Theta_n \in \text{Hom}^0(B_n, J_n)\) is an
isomorphism. To that end, we define:

\[ \bar{\Theta}_n := \sum_{m \mid n} \frac{\phi_{n,m}^*}{\deg \phi_{n,m}} = \sum_{m \mid n} \frac{m}{n} (\phi_{n,m}^*) \in \Hom^0(\mathcal{B}_n, \mathcal{J}_n). \]

Let \((m)_{m \mid n} \in \Hom(\mathcal{B}_n, \mathcal{B}_n)\) denote the \(K\)-isogeny given by multiplication-by-\(m\) on each \(A_m\). Then

\[ \Theta_n = \bar{\Theta}_n \cdot (m)_{m \mid n} \in \Hom^0(\mathcal{B}_n, \mathcal{J}_n). \]

so it suffices to prove that: \(\bar{\Theta}_n \in \Hom^0(\mathcal{B}_n, \mathcal{J}_n)\) is an isomorphism. To see this, fix \(n \in \mathbb{N}\), take any \(m \mid n\), let \(\pi_{n,m} : \mathcal{B}_n \rightarrow \mathcal{B}_m\) be the natural projection, and consider the following diagram of \(\text{Isog}_K:\)

\[ \begin{array}{ccc}
\mathcal{B}_n & \xrightarrow{\pi_{n,m}} & \mathcal{B}_m \\
\bar{\Theta}_n \downarrow & & \downarrow \bar{\Theta}_m \\
\mathcal{J}_n & \xrightarrow{(\phi_{n,m})_*} & \mathcal{J}_m.
\end{array} \]

(11.11)

Suppose \(d\) is any divisor of \(n\). If \(d\) also divides \(m\), then we have

\[ \bar{\Theta}_m \cdot \pi_{n,m} = \frac{d}{m}(\phi_{m,d}^*) = (\phi_{n,m})_* \cdot \bar{\Theta}_n \in \Hom^0(\mathcal{A}_d, \mathcal{J}_m). \]

One the other hand, if \(d\) does not divide \(m\), then Lemma 11.5 says that

\[ \bar{\Theta}_m \cdot \pi_{n,m} = 0 = (\phi_{n,m})_* \cdot \bar{\Theta}_n \in \Hom^0(\mathcal{A}_d, \mathcal{J}_m). \]

Thus, we have \(\bar{\Theta}_m \pi_{n,m} = (\phi_{n,m})_* \bar{\Theta}_n \in \Hom^0(\mathcal{A}_d, \mathcal{J}_m)\) for every divisor \(d\) of \(n\), and it follows that the diagram (11.11) commutes. The projections \(\pi_{n,m}\) arrange the \(\mathcal{B}_n\)'s into an inverse system, and the commutativity of (11.11) implies that the \(\bar{\Theta}_m\)'s extend to a morphism of the respective inverse limits:

\[ \lim_{m \mid n} \bar{\Theta}_m : \prod_{m \mid n} \mathcal{A}_m = \lim_{m \mid n} \mathcal{B}_m \rightarrow \lim_{m \mid n} \mathcal{J}_m. \]

(11.12)

This morphism fits into the following commutative diagram in \(\text{Isog}_K\):

\[ \begin{array}{ccc}
1 & \rightarrow & \mathcal{A}_n \\
\downarrow & & \downarrow \bar{\Theta}_n \\
\lim_{m \mid n} \mathcal{A}_m & \xrightarrow{\lim_{m \mid n} \pi_{n,m}} & \prod_{m \mid n} \mathcal{A}_m \\
\downarrow & & \downarrow \lim_{m \mid n} \bar{\Theta}_m \\
1 & \rightarrow & \mathcal{J}_n \\
\downarrow & & \downarrow \lim_{m \mid n} \pi_{n,m} \\
\lim_{m \mid n} \mathcal{J}_m.
\end{array} \]

(11.13)

in which the rows are exact. Now, we show that \(\bar{\Theta}_n\) is an isomorphism by (strong) induction on \(n\). The base-case \(n = 1\) is trivial, since \(\mathcal{A}_1 = \mathcal{B}_1 = \mathcal{J}_1\) and \(\bar{\Theta}_1\) is simply the identity. Next, suppose we have some \(n \geq 2\) such that \(\bar{\Theta}_m\) is an isomorphism for every \(m < n\). Then, the right vertical arrow in (11.13) is an isomorphism, so we may apply the Snake Lemma to conclude that the middle arrow \(\bar{\Theta}_n\) has trivial kernel and co-kernel, and hence, is an isomorphism.

\[ \square \]

**Remark 11.14.** We note in passing that \(\bar{\Theta}_n\), being an isomorphism in \(\text{Isog}_K\), implies after the fact that the bottom right arrow of (11.13) is surjective.
12. Second Reduction: From $[W^*_n]$ to $[V^*_n]$

12.1. In this section, we assume for simplicity that $k$ is algebraically closed; this does not pose any issues because the main result of this section, Proposition 12.2 below, continues to hold provided that $k$ contains the appropriate root of unity (needed to consider the spaces $W^*_n$ and $\tilde{W}^*_n$).

For each $n \in \mathbb{N}$ and $\bullet \in \{\text{cyc, re, im, dh}\}$, we denote the new part of $\mathbb{J}^*_n/K$ (the Jacobian of $\mathbb{X}^*_n/K$) by $\mathbb{A}^*_n/\mathbb{K}$, and we denote by

$$\Theta^*_n : \mathbb{E}^*_n \longrightarrow \mathbb{J}^*_n$$

the new parts decomposition provided by Lemma 11.8.

Fix $n \geq 2$ and $\bullet \in \{\text{cyc, re, im}\}$. Let $\mathbb{K}$ denote the corresponding field in Table 9.3. Observe from the proof of Theorem 9.17 (a) that for $i = 1, \ldots, r$, the point $Q^*_i \in \mathbb{X}^*_n(\mathbb{K})$ generates a torsor (cf. 2.7) under the cyclic group

$$G_{i,n} := \langle \sigma_{i,n} \rangle \subset \text{Gal}(\mathbb{K}/\mathbb{K}_1).$$

So, for each $i$ the space $W^*_i$ from 9.10 is free of rank one over the group algebra $\mathbb{Q}G_{i,n} = \text{span}_{\mathbb{Q}} \{1, \sigma_{i,n}, \ldots, \sigma_{i,n}^{n-1}\}$, which we identify with the commutative ring $\mathbb{Q}[z]/(z^n - 1)$ in the obvious way. Recall the inverse cyclotomic polynomial $\Psi_n(x)$ from (2.8). Since $\sigma_{i,n}$ fixes $D_\infty$, we have $\Psi_n(\sigma_{i,n})D_\infty = \Psi_n(1)D_\infty = 0$. It follows that the divisor

$$\Psi_{i,n} := \Psi_n(\sigma_{i,n})Q^*_i = \Psi_n(\sigma_{i,n})Q^*_i \in \text{Div}^0(\mathbb{X}^*_n)_{\mathbb{K}}$$

lies in $W^*_i$. We define for each $i$ the subspace (as in (2.9)):

$$V^*_i := \text{span}_{\mathbb{Q}G_{i,n}} \{Q^*_1, \ldots, Q^*_r\} \subset W^*_i.$$

Adding these subspaces up for $i = 1, \ldots, r$, we obtain the subspace

$$V^*_n := V^*_1 \oplus \cdots \oplus V^*_r \subset W^*_n.$$

To complete the picture, we define

$$V^*_1 = W^*_1 \subset \mathbb{J}^*_1(\mathbb{K})_Q = \mathbb{J}(\mathbb{K})_Q.$$

In the next proposition, we observe that there is a decomposition of $[W^*_n]$ into the direct sum $\Theta_m|n[V^*_m]$ which mirrors the new parts decomposition of $\mathbb{J}^*_n$.

**Proposition 12.2.** For any $n \in \mathbb{N}$ and $\bullet \in \{\text{cyc, re, im}\}$, we have the following.

(a) The embedding $[V^*_n] \hookrightarrow \mathbb{J}^*_n(\mathbb{K})_Q$ has image contained in $\mathbb{A}^*_n(\mathbb{K})_Q$.

(b) The new parts decomposition $\Theta^*_n : \mathbb{E}^*_n \longrightarrow \mathbb{J}^*_n$ induces a $\mathbb{Q}$-isomorphism

$$\Theta^*_n : \bigoplus_{m|n} [V^*_m] \rightarrow [W^*_n] \subset \mathbb{J}^*_n(\mathbb{K})_Q.$$

Consequently, if we write $\rho^*_n$ for the dimension of $[V^*_n]_Q$, we have

$$R^*_n = \sum_{m|n} \rho^*_m.$$

**Proof.** For part (a), start by fixing $i \in \{1, \ldots, r\}$. Let $m$ be any divisor of $n$, and observe that $\phi^*_{n,m}(Q^*_i) = Q^*_i \in \mathbb{X}^*_m(\mathbb{K}_m)$. In fact, $Q^*_i$ is a $\mathbb{K}_m$-point of $\mathbb{X}^*_m$, and since the restriction of $\sigma_{i,m} \in \text{Aut}_{\mathbb{K}}(\mathbb{K}_m)$ to the subfield $\mathbb{K}_m$ is the automorphism $\sigma_{i,m} \in \text{Aut}_{\mathbb{K}}(\mathbb{K}_m)$, we have $\sigma_{i,n}Q^*_i = \sigma_{i,m}Q^*_i$. Thus, for any $j \in \mathbb{Z}$ we have

$$\sigma_{i,n}^j Q^*_i \xrightarrow{\phi^*_{n,m}} \sigma_{i,m}^j Q^*_i = \sigma_{i,m}^j Q^*_i \in \mathbb{X}^*_m(\mathbb{K}).$$
It follows that the pushforward map \((\phi_{n,m}^\bullet)_*\) on divisors (over \(\mathbb{K}_n\)) satisfies

\[
\Psi_{i,n}^\bullet \xrightarrow{(\phi_{n,m})_*} \Psi_m(\sigma_{i,m})Q_{i,m}^\bullet \in \text{Div}^0 \mathbb{X}_m^\bullet(\mathbb{K}_n).
\]

Now, if \(m < n\), then \(m/e\) divides \(\Psi_n(x)\) in \(\mathbb{Q}[x]\) (cf. the definition of \(\phi_n(x)\) in (2.8)). Thus, we have \(\Psi_n(\sigma_{i,m}) = 0 \in \mathbb{Z}G_{i,m}\), giving

\[
[\Psi_{i,n}^\bullet] \xrightarrow{(\phi_{n,m})_*} [\Psi_m(\sigma_{i,m})Q_{i,m}^\bullet] = 0 \in \mathbb{J}_m^\bullet(\mathbb{K}_n).
\]

By letting \(m\) range over the divisors of \(n\) less than \(n\), we find that \([\Psi_{i,n}^\bullet]\) is the kernel of each push-forward map \((\phi_{n,m}^\bullet)_*\), and since \(A_n^\bullet\) is the connected component of the intersections of these kernels, we conclude that some multiple of \([\Psi_{i,n}^\bullet]\) is contained in \(A_n^\bullet(\mathbb{K}_n)\). This implies that \([V_{i,n}^\bullet]\) is contained in \(A_n^\bullet(\mathbb{K}_n)\mathbb{Q}\), and finally, by allowing \(i\) to range over \(\{1, \ldots, r\}\), we conclude that \([V_{i,n}^\bullet]\) is also contained in \(A_n^\bullet(\mathbb{K}_n)\mathbb{Q}\), which concludes the proof of (a).

We turn now to the proof of (b). Observe that the inverse system \((\mathbb{J}_n, (\phi_{n,m}^\bullet)_*)\) of abelian varieties gives rise an inverse system of \(\mathbb{Q}\)-vector spaces \(([W_n^\bullet], (\phi_{n,m}^\bullet)_*)\). For \(n \in \mathbb{N}\), consider the natural representation of \(\prod_{i=1}^r G_{i,n} = \text{Gal}(\mathbb{K}_n/\mathbb{K}_1)\) on \([W_n^\bullet] = \sum_{i=1}^r [W_{i,n}^\bullet]\). For each \(i\), the subspace \([V_{i,n}^\bullet]\) is an invariant subspace on which \(\sigma_{i,n}\) acts by multiplication by a primitive \(n\)-th root of unity on \(\Omega_{i,n}\), i.e. \([V_{i,n}^\bullet]\) decomposes as the product \(\bigotimes_x V_x\), where \(x\) ranges over the \(\phi(n)\)-many embeddings \(Z_N \hookrightarrow \mathbb{C}^\times\). For any \(m\mid n\), the homomorphism \((\phi_{n,m}^\bullet)_* : [V_m^\bullet] \hookrightarrow [W_{i,n}^\bullet]\) is an embedding whose image is similarly the invariant subspace on which \(G_{i,n}\) acts by multiplication by a primitive \(m\)-th root of unity. As we range over all \(m\) dividing \(n\), the direct sum of the subspaces \([V_{i,m}^\bullet]\) equals \([W_{i,n}^\bullet]\). Summing over \(i = 1, \ldots, r\), we conclude that

\[
\bigoplus_{m|n} [V_m^\bullet] = \bigoplus_{m|n} \sum_{i=1}^r [V_{i,n}^\bullet] \xrightarrow{\sim} \sum_{i=1}^r [W_{i,m}^\bullet] = [W_n^\bullet].
\]

We conclude this section with a last lemma to simplify the task of determining the integers \(\rho_n^\bullet\).

**Lemma 12.3.** Let \(n \geq 2\), and let \(\bullet \in \{\text{cyc}, \text{re}, \text{im}\}\). Then, the natural addition map

\[
[V_{1,n}^\bullet] \oplus \cdots \oplus [V_{r,n}^\bullet] \rightarrow [V_n^\bullet]
\]

is an isomorphism of \(\mathbb{Q}\)-vector spaces. Consequently, \(\rho_n^\bullet = r \phi(n)\) if and only if \([\Psi_{1,n}^\bullet]\) \(\in \mathbb{J}_n^\bullet(\mathbb{K}_n)\) is a point of infinite order for each \(i = 1, \ldots, r\).

**Proof.** Note first that for each \(i\), since \([V_{i,n}^\bullet]\) is annihilated by \(\Phi_n(\sigma_{i,n})\), Lemma 2.10 implies that it is either trivial or free of rank one over \(\mathbb{Q}(\zeta_n) = \mathbb{Q}[\sigma_{i,n}]/\Phi_n(\sigma_{i,n})\), with the latter being the case if and only if \([\Psi_{1,n}^\bullet]\) \(\in \mathbb{J}_n^\bullet(\mathbb{K}_n)\). Suppose for a contradiction, then, that we have elements \(m_i \in [V_{i,n}^\bullet]\), with \(m_i = 0\) for some \(e\), such that \(m_1 + \cdots + m_r = 0[V_n^\bullet]\). Observe that \(\sigma_{e,n}\) acts trivially on \(m_i\) for \(i \neq e\), since it acts trivially on the point \(\Omega_{i,n}\), for \(i \neq e\). Thus, multiplying the relation \(\sum_i m_i = 0\) by \((\sigma_{e,n} - 1)\) results in the relation \((\sigma_{e,n} - 1)m_e = 0 \in [V_{e,n}^\bullet]\). This forces \([V_{e,n}^\bullet]\) \(= 0\), a contradiction.

13. Determining \(\rho_n^\text{cyc}, \rho_n^\text{re},\) and \(\rho_n^\text{im},\) and finishing the proof of Theorem 9.17

In this section, we finish up the proof of Theorem 9.17 (b) by determining the integers \(\rho_n^\bullet = \text{dim}_\mathbb{Q}[V_n^\bullet]\), for \(\bullet \in \{\text{cyc}, \text{re}, \text{im}\}\). Since this integer is geometric in nature (i.e. it does not change upon extensions of the ground field \(k\)), we again assume without loss of generality for this section that \(k\) is algebraically closed.
There is a trivial case when $\rho_n^* = 0$, namely, if $n$ and $d$ are small enough that $\dim A_n^* = 0$. It turns out that if $d$ and $n$ are large enough that $\dim A_n^* > 0$, then there are essentially only two distinct scenarios:

- For $n = 1$, we have $X_1^{\text{cyc}} = X_1^{\text{re}} = X$ (the original curve in 4.4), and for $i = 1, \ldots, r$, we have $Q_{i,1}^{\text{cyc}} = Q_{i,1}^{\text{re}} = (u_i, v_i)$ (the points in (4.7)). In this case the equality

$$\dim_Q [V_1^{\text{cyc}}] = \dim_Q [V_1^{\text{re}}] = r - 1$$

was proved by Shioda in [Shi98, Theorems 4, 5] (as we mentioned in 4.4). We show that similarly that $\dim_Q [V_1^{\text{im}}] = r$.

- For $n \geq 2$, we show using the tools in Section 2 that each $[A_i^*] \in \mathbb{J}_n(\mathbb{K}_n)$ is of infinite order, which implies that the maximum possible dimension $\rho_n^* = r\phi(n)$ is attained.

**Theorem 13.1.** Each integer $\rho_n^* = \dim_Q [V_n^*]$ is given by the values in the table below.

| $\rho_n^{\text{cyc}} = \rho_n^{\text{re}} = \rho_n^{\text{im}}$ | $d = 1$ | $d = 2$ | $d \geq 3$ |
|-------------------------------------------------|---------|---------|-----------|
| $n = 1$ | 0       | 0       | 4$\phi(n)$|
| $n = 2$ | 0       | 6$\phi(n)$| $r - 1$   |
| $n \geq 3$ | 4$\phi(n)$ | 6$\phi(n)$ | $r \phi(n)$ |

**Table 13.2:** Dimension of $[V_n^{\text{cyc}}]$, $[V_n^{\text{re}}]$, and $[V_n^{\text{im}}]$

**Proof.** We have $g_n^{\text{cyc}} = g_n^{\text{re}}$, and these equal 0 if and only if $(n, d) = (1, 1), (1, 2), (2, 1)$ (note: $g_n^{\text{im}} = g_n^{\text{re}} + 1$, and this never equals 0). If $d = 1$, then $\dim A_2^{\text{im}} = g_2^{\text{im}} - g_1^{\text{im}} = 1 - 1 = 0$. In all these cases the equality $\dim_Q [V_n^*] = 0$ is forced for the trivial reason that the ambient abelian variety $A_n^*$ is of dimension zero.

Next, let us show that $\dim_Q [V_1^{\text{im}}] = r$ for all $d \geq 1$. To ease notation, write $Q_i$ for $Q_{i,1}^{\text{im}}$ and put $\Omega_i := \Omega_{i,1}^{\text{im}} = 2Q_i - D_{\infty}$ so that, by definition, $[V_1^{\text{im}}] = \Omega_{1,1}^{\text{im}}$. We want to show that these points are linearly independent. Suppose for a contradiction that they are not, and that we have a non-trivial linear dependence relation

$$a_1[\Omega_1] + \cdots + a_r[\Omega_r] = 0 \in \mathbb{J}_1^{\text{im}}(\mathbb{K}_1),$$

in which $a_s \neq 0$ for some $s \in \{1, \ldots, r\}$. Here we have $\mathbb{K}_1 = \mathbb{K}_1^{\text{din}} = k(u_1^{\text{din}}, \ldots, u_r^{\text{din}})$. Recall from (8.6) that we have an involution $\delta_s := \delta_{s,1} \in \text{Aut}_K(\mathbb{K}_1)$ which sends $u_s^{\text{din}} \mapsto (u_s^{\text{din}})^{-1}$ and which fixes $u_i^{\text{din}}$ for $i \neq s$. Since $u_{i,1}^{\text{im}} = (u_{i,1}^{\text{re}}) - (u_{i,1}^{\text{din}})^{-1}$, we see that $\delta_s$ fixes $u_{i,1}^{\text{im}}$ for $i \neq s$, and $\delta_s$ sends $u_{i,1}^{\text{im}} \mapsto -u_{i,1}^{\text{im}}$. Since $Q_i = (u_{i,1}^{\text{re}}, v_i u_{i,1}^{\text{im}})$, we find that

$$\delta_s(Q_i) = \begin{cases} Q_i & \text{if } i \neq s, \\ iQ_i & \text{if } i = s, \end{cases}$$

which in turn implies that

$$\delta_s([\Omega_i]) = \begin{cases} [\Omega_i] & \text{if } i \neq s, \\ -[\Omega_i] & \text{if } i = s. \end{cases}$$

So, multiplying the relation (13.3) by $(\delta_s - 1)$, we obtain

$$(\delta_s - 1)a_s[\Omega_s] = -2a_s[\Omega_s] = 0 \in \mathbb{J}_1^{\text{im}}(\mathbb{K}_1).$$
So, \([\Omega_3]\) must be a torsion point. But since \(Q \in X_1^m(\mathbb{K}_1)\) is a transcendental point of \(X_1^m / K\), this contradicts Lemma 2.15, which asserts that \([\Omega_3]\) is of infinite order.

It remains only to consider the cases with \(n \geq 2\) in which \(\mathbb{A}_n^*\) is positive dimensional. We proceed now in two parts, depending on the genus \(g_n^*\) of \(\mathbb{A}_n^*\).

(i) The case \(g_n^* = 1\). We have \(g_n^m = 1\) if and only if \(nd = 2\), which holds when \((n, d) = (2, 1)\), and we have already dealt with this case. On the other hand, we have \(g_n^{oc} = g_n^p = 1\) if and only if \((n, d) = (3, 1)\), \((4, 1)\), or \((2, 2)\). Suppose we are in one of these three cases, so that \(n\) is a power of a prime \(p\) (i.e. \(p = 2\) or \(3\)), and assume for a contradiction that \(\dim_Q[V_{i,n}^*] < \phi(n)\). To ease notation, we everywhere drop the subscript "\(i, n\)" and superscript \(\bullet\) on the point \(Q_{i,n}^*\) and divisors \(\mathbb{P}_{i,n}^*\) and \(\Omega_{i,n}^*\). Put \(\tau := \sigma_{i,n}^{p/n} \in \text{Aut}_K(\mathbb{K}_n)\), which is an element of order \(p\). Lemma 2.10 says that \([\mathfrak{M}] = [(\tau - 1)Q] = (\tau - 1)[Q]\) is a torsion point of \(\mathbb{J}_n^*(\mathbb{K}_n)\). For \(j = 2, \ldots, p\), we have

\[
(\tau - 1)[\mathfrak{M}] = 2(1 + \tau \cdots + \tau^{j-1})[Q] = 0 \in \mathbb{J}_n^*(\mathbb{K}_n). \tag{13.4}
\]

The quotient by \(\langle \tau \rangle\) is the degree \(p\) cover \(\phi_{n,p}^*: X_n^* \rightarrow X_{n/p}^*\). The target here is of genus 0, so putting \(E := (1 + \tau + \cdots + \tau^{p-1})\Omega \in \text{Div}^0(X_{n/p}^* \mathbb{K}_n)\), we have

\[
2[E] = (1 + \tau + \cdots + \tau^{p-1})[\mathfrak{M}] = (\phi_{n,p}^*)^*(\phi_{n,p}^*)^*[\mathfrak{M}] = 0 \in \mathbb{J}_n^*(\mathbb{K}_n). \tag{13.5}
\]

So, (13.4) and (13.5) together imply that

\[
\text{span}_Q\{[\mathfrak{M}], \tau[\mathfrak{M}], \ldots, \tau^{p-1}[\mathfrak{M}]\} = \text{span}_Q\{[E], (\tau - 1)[\mathfrak{M}], \ldots, (\tau^{p-1} - 1)[\mathfrak{M}]\} = \{0\}.
\]

But this implies that \([\mathfrak{M}] \in \mathbb{J}_n^*(\mathbb{K}_n)\) is a torsion point, which again contradicts Lemma 2.15 since \(Q\) is a transcendental point of \(X_n^*/K\). This concludes the proof.

(ii) The case \(g_n^* \geq 2\). We will be done if we are able to apply Lemma 2.12 to the curve \(X_n^* / K\) and point \(Q_{i,n}^* \in X_n^*(\mathbb{K}_n)\). To that end, let us start by noting that in all three cases (real, cyclic, and imaginary), and for all \(d\) and \(n\), assumption (a1) of the lemma is satisfied- the point \(Q_{i,n}^*\) and its hyperelliptic conjugate \(\iota Q_{i,n}^*\) each generate distinct \(G_{i,n}\)-torsors in \(X_n^*(\mathbb{K}_n)\), i.e. the points \(\sigma_{i,n}^j Q_{i,n}^*\) and \(\iota \sigma_{i,n}^j Q_{i,n}^* \in X_n^*(\mathbb{K}_n)\) are all distinct. Again in all three cases and for all \(d\) and \(n\), assumption (a2) of the lemma is satisfied- since we have assumed \(k\) to be algebraically closed, Proposition 8.8 (c) says that \(K\) is algebraically closed in \(\mathbb{K}_n\), and Lemma 2.14 then says that we have an equality of torsion subgroups \(J_n^*(\mathbb{K}_n)_{\text{tors}} = J_n^*(K)_{\text{tors}}\). Recall now that the third (and final) assumption (a3) of Lemma 2.12 requires that \(g_n^* \geq \max\{2, 2^{\|n\|-1}\}\), where \(\|n\|\) denotes the number of distinct prime factors of \(n\). Assumption (a3) automatically holds if \(n\) is a prime power so we need only consider the case when \(\|n\| \geq 2\). In this case, using the fact that \(g_n^{oc} = g_n^{im} = g_n^m - 1 = (nd - 1 - [nd])/2\) (recall that \([nd]\) \(\in \{0, 1\}\) denotes the remainder of \(nd\) mod 2), we have the chain of inequalities

\[
g_n^* \geq (nd - 1 - [nd])/2
\]

\[
\geq (nd - 2)/2
\]

\[
\geq (n/2) - 1
\]

\[
\geq (2^{\|n\|-1} - 3)/2 - 1
\]

\[
= 2^{\|n\|-1}(1 + 1/2) - 1
\]

\[
= 2^{\|n\|-1} + (2^2 - 2 - 1)
\]

\[
\geq 2^\|n\|-1
\]

Thus, if \(g_n^* \geq 2\) then assumption (a3) of Lemma 2.12 is satisfied and the lemma implies that \(\dim_Q[V_{i,n}^*] = \phi(n)\). \(\square\)
13.6. **Proof of Theorem 9.17.** Fix the integers \(d\) and \(n\), and fix the label \(\bullet \in \{\text{cyc, re, im}\}\). Then, one checks that the values of \(P^*_n\) proved in Theorem 13.1, together with the identity \(\sum_{m|n} \phi(m) = n\), imply that \(R^*_n = \sum_{m|n} \dim_{\mathbb{Q}}[V^*_m]\) equals the value asserted in Table 9.18. Finally, the validity of Theorem 9.17 (b) follows from Lemma 10.7.

14. **Non-isotriviality of the Real, Imaginary, and Dihedral Families**

The main result of this section is the following proposition (which was already used in the proof of Theorem 1.3).

**Proposition 14.1** (Proved in 14.5). Any curve in the real, imaginary, and dihedral families in Table 9.3 is non-isotrivial over \(K = k(h)\) (provided, of course, that its genus is positive).

We will prove the proposition with the help of two lemmas. For simplicity, and without loss of generality, we assume throughout that \(k\) is algebraically closed.

**Lemma 14.2.** Let \(\phi : X \rightarrow Y\) be a cover of nice curves over \(K\). If \(Y/K\) is non-isotrivial of genus \(g > 1\), then \(X/K\) is also non-isotrivial.

**Proof.** Assume for a contradiction that \(Y/K\) is non-isotrivial of genus \(g > 1\) but \(X/K\) is isotrivial. Choose a suitable smooth \(k\)-variety \(V\) with function field \(K\) and spread out the cover \(\phi : X \rightarrow Y\) to a finite \(V\)-morphism \(\hat{\phi} : \hat{X} \rightarrow \hat{Y}\). For any point \(P \in V(k)\), this specializes to a cover \(\hat{\phi}_P : \hat{X}_P \rightarrow \hat{Y}_P\) of curves over \(\overline{k}\). By assumption, as we vary the geometric point \(P \in V(\overline{k})\), the curves \(\hat{X}_P/\overline{k}\) are all isomorphic to a fixed curve \(X/\overline{k}\), whereas \(\hat{Y}_P/\overline{k}\) varies over infinitely many isomorphism classes of genus \(g\) curves. But this is absurd– if \(g > 2\), then \(X/\overline{k}\) would cover infinitely many non-isomorphic curves of genus \(g > 2\), which contradicts a classical theorem of de Franchis (see [Kan86]), whereas if \(Y\) is of genus one then the Jacobian of \(X/\overline{k}\) would contain infinitely many elliptic curves over \(\overline{k}\) in its isotypic decomposition. \(\Box\)

Below, for an element \(\alpha \in \overline{k}\), we write \([\alpha]\) to denote the corresponding geometric point on \(\mathbb{A}^1_{\overline{k}} = \mathbb{P}^1_{\overline{k}} - \{\infty\}\).

**Lemma 14.3.** Let \(F(x) \in K[x]\) be a separable polynomial of degree at least 5, and let \(G\) denote its Galois group. Assume that the hyperelliptic curve

\[
\mathbb{Y}/K : y^2 = F(x)
\]

is isotrivial. Then, there exists a group embedding

\[
\theta : G \hookrightarrow \text{Aut}_{\overline{k}}(\mathbb{P}^1_{\overline{k}}), \quad g \mapsto \theta_g,
\]

such that for every root \(\alpha\) of \(F\) in \(\overline{k}\), we have \(\theta_g([\alpha]) = [g(\alpha)]\). In particular, if \(F(x)\) has a root in \(k\) or \(\deg F(x)\) is odd, then \(G\) is cyclic.

**Proof.** By assumption, there exists a curve \(Y/k\) and a \(\overline{k}\)-isomorphism \(\varphi : Y_{\overline{k}} \overset{\sim}{\rightarrow} \mathbb{Y}\). Then \(Y/k\) is hyperelliptic and admits a double cover \(\pi_Y : Y \rightarrow \mathbb{P}^1_k\). Thus, there is an isomorphism \(f_{\varphi} : \mathbb{P}^1_{\overline{k}} \overset{\sim}{\rightarrow} \mathbb{P}^1_{\overline{k}}\) which makes the following diagram commute:

\[
\begin{array}{ccc}
Y_{\overline{k}} & \xrightarrow{\varphi} & \mathbb{Y} \\
\pi_Y \downarrow & & \downarrow \pi_{\mathbb{Y}} \\
\mathbb{P}^1_{\overline{k}} & \xrightarrow{f_{\varphi}} & \mathbb{P}^1_{\overline{k}}
\end{array}
\]
We have a natural action of the Galois group $G_K := \text{Gal}(\overline{K}/K)$ on $\mathbb{P}^1_K$ in which every element $g \in G_K$ fixes $\infty$ and sends a point $[\alpha] \in \mathbb{P}_K^1 - \{\infty\}$ to $[g(\alpha)]$. We define the map (of sets)

$$\theta : G_K \longrightarrow \text{Aut}_K(\mathbb{P}_K^1), \quad g \longmapsto g \circ f_\psi \circ g^{-1} \circ f_\psi^{-1}. \tag{14.4}$$

Let $\alpha$ be a root of $F(x)$, so that $[\alpha]$ is a branch point of $\pi_Y$ and $P := f_\psi^{-1}[\alpha]$ is a branch point of $\pi_Y$. Since $P$ is fixed by $G_K$, we have

$$\theta_g([\alpha]) = g \circ f_\psi \circ g^{-1}(P) = g \circ f_\psi(P) = [g(\alpha)].$$

For every $g$ and $h$ in $G_K$, the element $\theta_{gh}$ agrees with the element $\theta_g \theta_h$ when restricted to the branch locus of $\pi_Y$, and since any automorphism of the projective line is determined by its effect on three points, it follows that $\theta_{gh} = \theta_g \theta_h$. Thus, $\theta : G \longrightarrow \text{Aut}_K(\mathbb{P}_K^1)$ is a group homomorphism. Visibly, $\theta_g$ is the identity if and only if $g$ fixes all the roots of $F(x)$. Thus, it factors through the Galois group of $F(x)$ to give a group embedding $\theta : G \longhookrightarrow \text{Aut}_K(\mathbb{P}_K^1)$ satisfying $\theta_g([\alpha]) = [g(\alpha)]$ for every root $\alpha$ of $F(x)$.

For the second statement, assume that $F(x)$ has a root $a \in k$, or that deg $F$ is odd. In the latter case, let $P := \infty$, and in the former case let $P := [a]$. Then the image of $G$ under $\theta$ is a finite subgroup of $\text{Aut}_K(\mathbb{P}_K^1)$ which fixes $P$. So, if $f : \mathbb{P}_K^1 \longrightarrow \mathbb{P}_K^1$ denotes the quotient by $G$, then $P$ is totally ramified under $f$ and $G$ is its inertia group. But since char $k = 0$, the ramification is necessarily tame and the inertia group of $P$ must be cyclic (see [Sta18, Lemma 09EE]).

14.5. Proof of Proposition 14.1. For all $d \geq 1$, the curve $X_4^\text{en}/K$ is non-isotrivial because any hyperelliptic curve $X/k$ of genus $g_1^\text{en}$ arises as a specialization because, given a double cover $\pi : X \longrightarrow \mathbb{P}_k^1$, we can choose the coordinate on $\mathbb{P}_k^1$ in such a way that $2$, $-2$, and $\infty$ are all branch points of $\pi$, and such a curve is visibly a specialization of $X_1^\text{en}$. Since there exist covers $\psi_n^\text{en} : X_n^\text{an} \longrightarrow X_n^\text{en}$ and $\phi_n^\text{en} : X_n^\text{en} \longrightarrow X_1^\text{en}$, Lemma 14.2 implies that $X_n^\text{en}/K$ is non-isotrivial for all $d \geq 1$ and $n \in \mathbb{N}$.

By a similar argument, the curves $\tilde{X}_4^\text{en}/K$ and $\tilde{X}_1^\text{en}/K$ are non-isotrivial if $d \geq 2$, and it follows again from Lemma 14.2 that $\tilde{X}_n^\text{en}/K$, $\tilde{X}_n^\text{en}/K$, and $\tilde{X}_n^\text{an}/K$ are non-isotrivial for all $n \in \mathbb{N}$ and $d \geq 2$.

Suppose next that $d = 1$. If $n = 2$ or $3$ then $\tilde{X}_n^\text{en}/K$ and $\tilde{X}_n^\text{en}/K$ are both elliptic curves, and one checks that their $j$-invariant lies in $K \setminus k$. If $n \geq 4$, then $\tilde{X}_n^\text{en}$ and $\tilde{f}_n^\text{en}$ are both separable of degree $n + 1 \geq 5$ having a root in $k$, and their Galois group over $K$ is dihedral of order $2n$. So in this case Lemma 14.3 implies that $\tilde{X}_n^\text{en}/K$ and $\tilde{X}_n^\text{en}/K$ are non-isotrivial. Again, Lemma 14.2 implies that for $d = 1$ and $n \geq 2$, $\tilde{X}_n^\text{an}/K$ is non-isotrivial (note: it is of genus zero when $d = n = 1$).

It remains only to prove the statement for the curves $X_n^\text{en}/K$. If $d \geq 3$ then $X_n^\text{en} = 0$ (the original curve from Mestre’s construction 4.4). This is non-isotrivial over $K$, and so the same is true of $X_n^\text{en}/K$ for all $n \in \mathbb{N}$ by Lemma 14.2.

Next, suppose that $d = 2$. If $n = 2$, then the double cover $\tilde{\phi}_2^\text{en} : X_2^\text{en} \longrightarrow \tilde{X}_2^\text{en}$ implies by Lemma 14.2 that $X_2^\text{en}/K$ is non-isotrivial. If $n \geq 3$ then $\tilde{f}_n^\text{en}(x) = \psi(f_n^\text{en}(x))$ is of degree $n d \geq 6$. If $a_1$ and $a_2$ denote the roots of $\psi(x)$ in $\overline{K}$, then $\tilde{f}_n^\text{en}(x)$ factors as $h_2(f_n^\text{en}(x) - a_1)(f_n^\text{en}(x) - a_2) \in \overline{K}[x].$ The Galois group of each factor contains the cyclic group $Z_n$ (cf. 7.4), which implies that the Galois group $G$ of $\tilde{f}_n^\text{en}(x)$ contains $Z_n \times Z_n$. Applying Lemma 14.3, we find that if $X_n^\text{en}/K$ is isotrivial then $G$ is a subgroup of $\text{Aut}_K(\mathbb{P}_K^1)$. This is impossible because $\text{Aut}_K(\mathbb{P}_K^1)$ does not contains $Z_n \times Z_n$, for $n \geq 3$. We conclude that if $d = 2$ and $n \geq 2$, then $X_n^\text{en}/K$ is non-isotrivial.

Finally, suppose that $d = 1$. If $n = 3$ then $X_n^\text{en}/K$ is the elliptic curve $y^2 = h_1(f_3^\text{en}(x)) + h_0$, and one can check that its $j$-invariant lies in $K \setminus \overline{k}$. If $n = 4$ then the double cover $\tilde{\phi}_4^\text{en} : X_4^\text{en} \longrightarrow \tilde{X}_2^\text{en}$ together with Lemma 14.2 implies that $X_4^\text{en}/K$ is non-isotrivial. If $n \geq 5$ is odd, then $\tilde{f}_n^\text{en}(x)$ is odd
of degree $n$ and has Galois group $D_n$ over $K$, so Lemma 14.3 implies that $\mathbb{X}_n^{re}/K$ is non-isotrivial. Now, any integer $n \geq 3$ is either a power of two, in which case we have the cover $\phi_{n,4}^{re}: \mathbb{X}_n^{re} \to \mathbb{X}_4^{re}$, or else $n$ is divisible by an odd prime $p$, in which case we have the cover $\phi_{n,p}^{re}: \mathbb{X}_n^{re} \to \mathbb{X}_p^{re}$. So, we conclude by Lemma 14.2 that if $d = 1$ and $n \geq 3$, then $\mathbb{X}_n^{re}/K$ is non-isotrivial. This concludes the proof.

15. Complex multiplication of $A_n^{cyc}/K$ and the proof of Theorem 1.13

For this section, we set $d = 1$, so that the polynomial $\xi_n^{cyc}(x)$ from Table 9.3 is $h(x^n) = h_1 x^n + h_0$, and the associated hyperelliptic curve is $\mathbb{X}_n^{cyc}/K: y^2 = h_1 x^n + h_0$. For any $P = (a, b) \in A^2(k)$ such that $ab \neq 0$, the specialized curve

$$X_n/k : y^2 = a(x^n + b)$$

(15.1)

is of the same genus as $\mathbb{X}_n^{cyc}$. For all $n$ and all $m$ dividing $n$, we have again the natural covers $\phi_{n,m}: \mathbb{X}_n \to \mathbb{X}_m$ defined by $(x, y) \mapsto (x^{n/m}, y)$ which make $(X_n, \phi_{n,m})$ into a $\hat{\mathbb{Z}}$-system of hyperelliptic curves over $k$. In particular, each cover $\phi_{n,1}: X_n \to X_1$ is the quotient (provided $k$ contains $\zeta_n$) by the order $n$ automorphism

$$\sigma_n : X_n \longrightarrow X_1, \quad (x, y) \mapsto (\zeta_n x, y).$$

Let $J_n/k$ denote the Jacobian of $X_n$, and let $A_n/k$ denote its new part. Then, by Lemma 11.8, we have $\dim A_n = 0$ if $n = 1$ or 2, and

$$\dim A_n = \phi(n)/2, \quad \text{if } n \geq 3.$$ 

Define the endomorphism

$$\overline{\sigma}_n : J_n \longrightarrow J_n, \quad [D] \longmapsto [(\sigma_n)_* D].$$

We show below that this endomorphism endows $A_n/k$ with complex multiplication by the number field $\mathbb{Q}(\zeta_n)$.

**Proposition 15.2.** Fix $n \geq 3$ (so that $X_n/k$ is of positive genus) and assume that $k$ contains $\zeta_n$. Then, the automorphism $\overline{\sigma}_n \in \text{Aut}_k(J_n)$ restricts to an automorphism $\overline{\zeta}: A_n \simeq A_n$ which satisfies

$$\Phi_n(\overline{\zeta}) = 0 \in \text{End}_k^0(A_n).$$

Consequently, the $\mathbb{Q}$-subalgebra $\mathbb{Q}[\overline{\zeta}] \subset \text{End}_k^0(A_n)$ is isomorphic to the cyclotomic field $\mathbb{Q}(\zeta_n)$ via the map $\overline{\zeta} \mapsto \zeta_n$, and $A_n$ has complex multiplication by $\mathbb{Q}(\zeta_n)$.

**Proof.** For any $m$ dividing $n$, we have the following commutative diagram of curves and an induced diagram of their Jacobians:

$$
\begin{array}{ccc}
X_n & \xrightarrow{\sigma_n} & X_n \\
\downarrow{\phi_{n,m}} & & \downarrow{\phi_{n,m}} \\
X_m & \xrightarrow{\sigma_m} & X_m
\end{array}
\quad
\begin{array}{ccc}
J_n & \xrightarrow{\overline{\sigma}_n} & J_n \\
\downarrow{\phi_{n,m}} & & \downarrow{\phi_{n,m}} \\
J_m & \xrightarrow{\overline{\sigma}_n} & J_m
\end{array}
$$

It follows at once that $\overline{\sigma}_n(A_n)$ is contained in the kernel of $(\phi_{n,m})_*$. By letting $m$ range over all divisors of $n$, it follows that $\overline{\sigma}_n(A_n) = A_n$, so $\overline{\sigma}_n$ indeed restricts to an automorphism $\overline{\zeta}$ of $A_n$. For every factorization $n = me$, with $m < n$, define the polynomial

$$q_m(x) := (x^n - 1)/(x^m - 1) = 1 + x^m + \cdots + (x^m)^{e-1} \in \mathbb{Z}[x],$$
and observe that \[(\phi_{n,m})^* \circ (\phi_{n,m})_* = q_m(\overline{\sigma}_n) \in \text{End}_k^n(J_n).\]

It follows that for any \(m\parallel n\), we have \(q_m(\overline{\xi}) = 0 \in \text{End}_k(A_n)\). It is an exercise to see that the gcd of the polynomials \(q_m(x)\), as \(m\) ranges over the divisors of \(n\) less than \(n\), is the cyclotomic polynomial \(\Phi_n(x)\). So, we have \(\Phi_n(x) = \sum_{m\parallel n} q_m(x) f_m(x)\), for some set of polynomials \(f_m(x) \in \mathbb{Q}[x]\). It follows that \(\Phi_n(\overline{\xi}) = 0 \in \text{End}_k(A_n)\). Thus, the \(\mathbb{Q}\)-subalgebra \(\mathbb{Q}[\overline{\xi}] \subseteq \text{End}_k^n(A_n)\) is isomorphic to \(\mathbb{Q}(\zeta_n)\), and since \(\dim A_n = \phi(n)/2\), we conclude that \(A_n\) has complex multiplication by \(\mathbb{Q}(\zeta_n)\). □

**Remark 15.3.** The proof above serves equally well to show that \(\mathbb{A}^\text{cyc}_n / \mathbb{K}^\text{cyc}_n\) also has complex multiplication by \(\mathbb{Q}(\zeta_n)\) (provided \(k\) contains \(\zeta_n\)).

We conclude this section (and also the article) with:

**15.4. Proof of Theorem 1.13.** Fix \(N \geq 3\), and a number field \(k\) which contains \(\zeta_N\). Consider the open subset \(V \subset \mathbb{A}^4_k(u_N^\text{cyc})\) defined by the condition \(m_0 h_0 h_1(\text{disc } n) \neq 0\). Let \(P \in V(k)\) be a point, and put \(a := h_1(P)\) and \(b := h_0(P)\). Then, the entire \(\mathbb{Z}\)-system \((X_n^\text{cyc}, \phi_{n,m}^\text{cyc})\) can be specialized to the \(\mathbb{Z}\)-system \((X_n, \phi_{n,m})\), where \(X_n/k : y^2 = ax^n + b\) is the specialization of \(X_n^\text{cyc}\) at \(P\) and the covers \(\phi_{n,m}\) are again defined by \((x, y) \mapsto (x^{n/m}, y)\). Writing \(J_n/k\) for the Jacobian of \(X_n/k\), and \(A_n/k\) for its new part, it follows that for all \(n \in \mathbb{N}\), the specialization homomorphism \(J_n^\text{cyc}(k_N) \longrightarrow J_n(k)\) restricts to a homomorphism \(\mathbb{A}^\text{cyc}_n(k_N) \longrightarrow A_n(k)\). Note that if \(n \geq 3\) then \(A_n/k\) has complex multiplication by \(\mathbb{Q}(\zeta_n)\) by Proposition 15.2.

Now, Theorem 3.4 gives a thin subset \(T \subset V(k)\) such that for all \(P \in V(k) \setminus T\) and all \(m \mid N\), the specialization homomorphism \(J_m^\text{cyc}(k_N) \longrightarrow J_m(k)\), and hence, also its restriction \(\mathbb{A}^\text{cyc}_m(k_N) \hookrightarrow A_m(k)\), is injective. By Theorem 13.1, we therefore have \(\text{rk } A_m(k) \geq 4\phi(n) = 8(\dim A_m)\). So, to complete the proof of Theorem 1.13, it remains only to show that:

**The image of \(S := V(k) \setminus T\) under the natural \(k\)-morphism \(f : V \longrightarrow B := \text{Spec } k[h_1, h_0]\) is not thin in \(B\).**

Suppose for a contradiction that this is not the case, i.e. that there exists a generically finite cover \(g : U \longrightarrow B\) admitting no rational section and satisfying \(g(U(k)) \supset f(S)\). Let \(\tilde{U}\) denote the fibered product \(V \times_B U\), so that the base-change \(\tilde{g} : \tilde{U} \longrightarrow V\) is a generically finite cover which satisfies \(\tilde{g}(\tilde{U}(k)) \supset S\). By shrinking \(V\) to a smaller open subset if necessary, we may assume that \(g\) and \(\tilde{g}\) are both dominant \(k\)-morphisms. Now, the generic fiber of \(g\) is of the form

\[
\bigcup_{i=1}^\ell \text{Spec } L_i \longrightarrow \text{Spec } K
\]

for some positive integer \(\ell\), where each \(L_i/K\) is an extension of degree at least 2 (this last condition is equivalent to the statement that \(g\) does not admit a rational section \(B \longrightarrow U\)). So, if we put \(\mathbb{L}_i := L_i \otimes_K \mathbb{K}_N^\text{cyc}\), then the generic fiber of \(\tilde{g}\) is

\[
\bigcup_{i=1}^\ell \text{Spec } \mathbb{L}_i \longrightarrow \text{Spec } \mathbb{K}_N^\text{cyc}.
\]

By Proposition 8.8 (c), \(K\) is algebraically closed in \(\mathbb{K}_N^\text{cyc}\), which implies that each \(\mathbb{L}_i/\mathbb{K}_N^\text{cyc}\) is a field extension of the same degree as \(L_i/K\). Thus, the cover \(\tilde{g} : \tilde{U} \longrightarrow V\) does not admit a rational section, which implies that \(S\) is a thin subset of \(V(k)\). But this implies that \(V(k) = T \cup S\) is thin, which is a contradiction because \(k\) is a number field (hence satisfies the Hilbert Property) and \(V\) is a rational \(k\)-variety. □
REFERENCES

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, Geometry of algebraic curves. Vol. I, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985. MR770932 ↑8

[Bea10] Arnaud Beauville, Finite subgroups of PGL2(K), Vector bundles and complex geometry, 2010, pp. 23–29. MR2681719 ↑17, 20

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, Néron models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 ↑11

[Cap95] Lucia Caporaso, Counting rational points on algebraic curves, 1995, pp. 223–229. Number theory, I (Rome, 1995). MR1452380 ↑6

[CUV12] Ricardo Conceição, Douglas Ulmer, and José Felipe Voloch, Unboundedness of the number of rational points on curves over function fields, New York J. Math. 18 (2012), 291–293. MR2928577 ↑6

[CHM97] Lucia Caporaso, Joe Harris, and Barry Mazur, Uniformity of rational points, J. Amer. Math. Soc. 10 (1997), no. 1, 1–35. MR1325796 ↑2

[CT20] Jean-Louis Colliot Thélène, Point générique et saut du rang du groupe de Mordell–Weil, Acta Arithmetica (2020), ↑11

[Elk06] Noam D. Elkies, Z28 in E(Q), etc., 2006. Email to the NMBRTHRY@LISTSERV.NODAK.EDU mailing list. ↑4

[Elk07] , Three lectures on elliptic surfaces and curves of high rank, 2007. Preprint. arXiv: 0709.2908. ↑4

[Elk09] , About the cover: rational curves on a K3 surface, Arithmetic geometry, 2009, pp. 1–4. MR2498052 ↑4

[Fal83] Gerd Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), no. 3, 349–366. MR718935 ↑1

[GLL15] Ofer Gabber, Qing Liu, and Dino Lorenzini, Hypersurfaces in projective schemes and a moving lemma, Duke Math. J. 164 (2015), no. 7, 1187–1270. MR3347315 ↑11

[Kan86] Ernst Kani, Bounds on the number of nonrational subfields of a function field, Invent. Math. 85 (1986), no. 1, 185–198. MR842053 ↑37

[Kul01] Leopoldo Kulesz, Jacobiennes de courbes algébriques de genre 2 et 3 de grand rang sur Q, J. London Math. Soc. (2) 63 (2001), no. 2, 288–298. MR1810130 ↑4

[Mes91a] Jean-François Mestre, Courbes elliptiques de rang ≥ 11 sur Q(t), C. R. Acad. Sci. Paris Sér. I Math. 313 (1991), no. 3, 139–142. MR1121576 ↑2, 12

[Mes91b] , Courbes elliptiques de rang ≥ 12 sur Q(t), C. R. Acad. Sci. Paris Sér. I Math. 313 (1991), no. 4, 171–174. MR1122689 ↑2, 12

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan, Geometric invariant theory, Third, Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994. MR1304906 ↑11

[Nér52] André Néron, Problèmes arithmétique et géométriques rattachés à la notion de rang d’une courbe algébrique dans un corps, Bulletin de la Société Mathématique de France 80 (1952), 101–166. MR0056951 ↑2

[Nér56] André Néron, Propriétés arithmétiques de certaines familles de courbes algébriques, Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III, 1956, pp. 481–488. MR0087210 ↑2

[Odo85] R. W. K. Odoni, The Galois theory of iterates and composites of polynomials, Proc. London Math. Soc. (3) 51 (1985), no. 3, 385–414. MR805714 ↑14

[Poo17] Bjorn Poonen, Rational points on varieties, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR3729254 ↑11

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, A heuristic for boundedness of ranks of elliptic curves, J. Eur. Math. Soc. (JEMS) 21 (2019), no. 9, 2859–2903. MR3985613 ↑2

[Ser97] Jean-Pierre Serre, Lectures on the Mordell-Weil theorem, Third Edition, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR1757192 ↑11
[Shi98] Tetsuji Shioda, *Constructing curves with high rank via symmetry*, Amer. J. Math. **120** (1998), no. 3, 551–566. MR1623420 ↑2, 3, 4, 12, 13, 27, 35

[Sta18] The Stacks Project Authors, *Stacks Project*, 2018. ↑38

[Sti84] Henning Stichtenoth, *Die Ungleichung von Castelnuovo*, J. Reine Angew. Math. **348** (1984), 197–202. MR733931 ↑8

[SU99] Tetsuji Shioda and Yumiko Umezu, *On Néron’s construction of curves with high rank. I*, Comment. Math. Univ. St. Paul. **48** (1999), no. 1, 35–47. MR1684766 ↑2

[TTV91] Walter Tautz, Jaap Top, and Alain Verberkmoes, *Explicit hyperelliptic curves with real multiplication and permutation polynomials*, Canad. J. Math. **43** (1991), no. 5, 1055–1064. MR1138583 ↑5

[Ulm07] Douglas Ulmer, *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields*, Invent. Math. **167** (2007), no. 2, 379–408. MR2270458 ↑6

[Wat15] Mark Watkins, *A discursus on 21 as a bound for ranks of elliptic curves over \( \mathbb{Q} \), and sundry related topics*, 2015. Available at [http://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf](http://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf). ↑2