SUBSTITUTION POLYNOMIALS AND THE DECOMPOSITION OF RATIONAL FUNCTIONS

ERIC LEVIN

Advisor: Danny Neftin
University of Michigan REU 2014

Contents

1. Introduction

1.1. Background.

An important tool for studying the value set of a polynomial $f(X)$ defined over a finite field F_q is to look at its associated substitution polynomial $f^*(X,Y) \in F_q[X,Y]$, defined as the difference $f(X) - f(Y)$. Roughly speaking, the size of the zero set of $f^*(X,Y)$ measures how much $f(X)$ fails to be injective. In [1] and [2], results are obtained relating the quadratic and cubic (respectively) factors of f^* to the decomposition of f through polynomials whose value sets are known. In [3], a partial classification of polynomials with minimal value sets is obtained through the use of substitution polynomials.

In this paper, we generalize the notion of a substitution polynomial by defining the polynomial $f^*(X,Y)$ when $f(X)$ is a rational function instead of a polynomial. We then use this generalized definition to study the relationship between quadratic factors of $f^*(X,Y)$ and the decomposition of $f(X)$. In addition to the results themselves, one of the goals of this paper is to illustrate the use of algebraic methods such as Galois theory to answer questions of this type.

1.2. Definitions and notation.

We begin by fixing some notation which will be used throughout this paper.

- k denotes the algebraic closure of a fixed finite field.
- X, Y will always denote indeterminates.

- $e(q|p)$ denotes the ramification index of a place q lying over a place p in some extension E/F. We will sometimes denote the ramification index of q over p by e_q, when the place p is clear from context.
- T_n denotes the n'th Chebychev polynomial.

Definition 1.1.

Let E_1, E_2 be elliptic curves, $\pi_i : E_i \to \mathbb{P}^1_k$ be projections onto P^1_k, and $\phi : E_1 \to E_2$ be an isogeny. A *sub-Lattes map* is a rational function $\Lambda : \mathbb{P}^1_k \to \mathbb{P}^1_k$ which satisfies the following commutative diagram:

$$\begin{tikzcd}
E_1 \arrow[r, "\phi"] \arrow[d, "\pi_1"] & E_2 \arrow[d, "\pi_2"] \\
\mathbb{P}^1_k \arrow[r, "\Lambda"] & \mathbb{P}^1_k
\end{tikzcd}$$

Throughout this paper Λ will denote a sub-Lattes map.

Definition 1.2.

Let f be a rational function defined over k. Write

$$f(X) = \frac{f_1(X)}{f_2(X)},$$

where f_1 and f_2 are coprime. Then the associated *substitution polynomial*, denoted $f^*(X, Y)$ or simply f^*, is defined as

$$f^*(X, Y) = f_1(X)f_2(Y) - f_2(X)f_1(Y).$$

1.3. **The main result.**

The primary goal of this paper is to prove the following:

Theorem 1.3. *Let $f(X)$ be a rational function defined over the algebraic closure of a finite field, let T_n denote the n'th Chebychev polynomial, and let Λ denote a sub-Lattes map. Then $f^*(X, Y)$ has an absolutely irreducible quadratic factor if and only if f factors through $T_n \circ \mu$ or $\Lambda \circ \mu$ for some linear fractional μ.*

What follows is an outline of the argument we will use to prove Theorem 1.3. The main idea is to view $f^*(X, Y)$ as a polynomial over $k(x, y)$, where the pair (x, y) is a zero of $f^*(X, Y)$ $k(x, y)^2$. Since this implies that $f(x) = f(y)$, we can then study the following field diagram to obtain information about the decomposition of $f(x)$:

$$\begin{tikzcd}
& k(x, y) \arrow[dl, dash] \arrow[dr, dash] & \\
k(x) \arrow[dr, dash] & & k(y) \arrow[dl, dash] \\
& k(x) \cap k(y) &
\end{tikzcd}$$

We can show that $k(x) \cap k(y) = k(h(x))$ for some rational function h. Eventually we can show that under our hypotheses, $h(x)$ must be equivalent to either a Chebychev polynomial or a sub-Lattes map up to a linear fractional.

The key tool to determining what h can be is ramification theory. Specifically, if we can obtain restraints on how the places of $k(h(x))$ ramify in $k(x)$, we significantly restrict the possible forms that $h(x)$ can take. In order to obtain these restraints we use the powerful Riemann Existence Theorem, which describes an explicit connection between a rational function's ramification structure and monodromy group. So if we determine $\mathrm{Gal}(k(x,y)/k(h(x))$ and then prove that it is the monodromy group of $h(x)$, we can use the Riemann Existence Theorem to describe $h(x)$. In fact, with the exception of a special edge case (dealt with at the end of the paper), we will show that the monodromy group of h is the dihedral group D_{2n}.

Our argument for proving the converse statement in Theorem 1.3 is not quite as involved. Essentially, we use the information about how $f(X)$ factors through T_n or Λ to construct a field diagram similar to the one above. The pair (x, y) is then used to construct the desired quadratic factor $q(X, Y)$, where $q(x, y) = 0$.

Now a word on the organization of this paper. Part 2 is devoted to setting up the machinery needed to prove Theorem 1.3. In section 2.1, we present several important theorems in algebraic number theory which will be used later. Section 2.2 consists of a single theorem, although one which requires many lengthy calculations to prove. Part 3 is where we study the decomposition of f in depth. In section 3.1 we achieve an explicit description of the ramification structure of $h(x)$. The results of this section divide the possibilities for what h can be into two cases, which end up corresponding with whether the Galois closure of $k(x)/k(h(x))$ has genus 0 or genus 1. The actual calculation of this genus is carried out in section 3.2. Finally, in section 3.3 we prove all the facts stated in 1.3.

2. Preliminaries

2.1. **Some useful theorems.**

The following theorems are mostly standard facts from algebraic number theory. The lone exception is the Riemann Existence Theorem, which is usually stated as a result on ramified coverings of Riemann surfaces. Instead, we use a version describing ramified coverings of curves over a field of positive characteristic. Proofs of these theorems can be found in the bibliography.

Theorem 2.1. *(Riemann Existence Theorem* [4]*) Let k be the algebraic closure of a finite field, and consider an extension $k(x)/k(t)$ where x, t are transcendental over k. Let L be the Galois closure of $k(x)/k(t)$ with Galois group $G = Gal(L/k(t)$. Then there exists a set of nontrivial generators $g_1, ..., g_m$ of G such that $g_1 \cdots g_m = 1$ if and only if there are m branch points $p_1, ..., p_m$ of $k(x)/k(t)$ such that the ramification of p_i in $k(x)$ corresponds to the cycle structure of g_i.*

Remark 2.2. This last statement means that each place of $k(x)$ lying above p_i corresponds to an orbit of g_i, and the ramification index of that place is equal to the size of the corresponding orbit.

Theorem 2.3. *(Riemann-Hurwitz Formula* [5]*) Let E/F be an extension of function fields, let g_E, g_F be the genus of E and F respectively, and let $[E : F] = n$. Furthermore, let Q be the set of ramified places of F/K, and for each $q \in Q$ let e_q denote the ramification index of q. Then*

$$2g_F - 2 = (2g_K - 2)n + \sum_{q \in Q}(e_q - 1).$$

Theorem 2.4. *(Abhyankar's Lemma* [5]*) Let L/F be a finite separable extension of function fields, and let F_1, F_2 be intermediate fields such that $L = F_1F_2$. Let p be a place of L lying over a place p_0 of F, and let $p_i = p \cap F_i$ for $i = 1, 2$. If either $p_1|p$ or $p_2|p$ is tame, then*

$$e(p|p_0) = lcm(\ e(p_1|p), e(p_2|p)\ ).$$

Theorem 2.5. *(The Fundamental Equality* [5]*)*
Let E be and extension of a function field F, p a place of F, and $q_1, ..., q_m$ all the places of E lying over p. If $f(p|q)$ is the degree of the residue class field of q over the residue class field of p, then

$$\sum_{i=1}^{m} e(q_i|p)f(q_i|p) = [E : F].$$

2.2. **A group-theoretic result.**

As the Riemann Existence Theorem relates the structure of the monodromy group of a rational function $h(x)$ to the ramification of the extension $k(x)/k(h(x))$, it is only natural that group theory enters the picture. The following result on generating sets of the dihedral group D_{2n} will be later be used to classify possible ramification types in such an extension.

We now fix some notation specific to this section. The following are all descriptions of elements of D_{2n}. For the sake of convenience and readability, we describe these elements purely geometrically:

- r: Rotation by one vertex.
- s: Flip along some fixed vertex.
- T_1: Element of the form r^k $(k \neq 0)$.
- T_2: Element of the form $r^k s$ when n is odd.
- T_{2a}: Element of the form $r^k s$ that fixes no vertices when n is even.
- T_{2b}: Element of the form $r^k s$ that fixes two vertices when n is even.

Lemma 2.6. *Define r, s to be generators of D_{2n} such that $|r| = n$ and $|s| = 2$. Let $\{g_i \mid 1 \leq i \leq m\}$ be a set of nontrivial generators of D_{2n} such that $g_1 \cdots g_m = 1$. For each g_i, define ind$(g_i) = n - \#(g_i)$, where $\#(g_i)$ denotes the number of orbits of g_i when viewed as an element of S_n. Under the constraint $\sum_{i=1}^{m}$ ind$(g_i) = 2n-2$, the only possible such sets are of the following form:*

1. *$r^k s, r^j, r^{k-j} s$ with $(j, n) = 1$;*
2. *$r^{\alpha_1} s, r^{\alpha_2} s, r^{\alpha_3} s, r^{\alpha_4} s$ with $\alpha_1 - \alpha_2 = \alpha_4 - \alpha_3$, and $(t_1 - s_1, ..., t_m - s_m, n) = 1$ where $\{t_i - s_i\}$ is the set of all differences for $t_i, s_i \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, $t_i \neq s_i$.*

Proof:
To prove our claim, we begin with some calculations that show the number of generators m is equal to 3 or 4.

Next, some useful identities involving the index of elements of different types:

ind$(T_1) = n - d$ where d is a divisor of n, $d \neq n$. When n is odd we have $2 < d < \frac{n}{2}$, and so $\frac{n}{2} < n - d < n - 2$. Hence

$$\frac{n}{2} < \text{ind}(T_1) < n - 2$$

if n is odd. Similarly, when n is even we have

$$\frac{n}{2} \leq \text{ind}(T_1) \leq n - 2.$$

$$\text{ind}(T_2) = n - \frac{n+1}{2} = \frac{n-1}{2}.$$

$$\text{ind}(T_{2a}) = n - \frac{n}{2} = \frac{n}{2}.$$

$$\text{ind}(T_{2b}) = n - (\frac{n}{2} + 1) = \frac{n}{2} - 1.$$

We first show that if n is odd, D_{2n} cannot have more than four nontrivial generators satisfying our constraints. If it does have four generators, they must all be of type T_2. Suppose there are four generators for D_{2n}. We divide into cases:

Case 1:

$$4\mathrm{ind}(T_1) > 2n > 2n-2.$$

Case 2:

$$3\mathrm{ind}(T_1)+\mathrm{ind}(T_2) > \frac{3n}{2}+\frac{n-1}{2} = 2n-\frac{1}{2} > 2n-2.$$

Case 3:

$$2\mathrm{ind}(T_1)+2\mathrm{ind}(T_2) > n+(n-1) = 2n-1 > 2n-2.$$

Case 4:

$$\mathrm{ind}(T_1)+3\mathrm{ind}(T_2) > \frac{n}{2}+\frac{3(n-1)}{2} = 2n-\frac{3}{2} > 2n-2.$$

Case 5:

$$4\mathrm{ind}(T_2) = 2(n-1) = 2n-2.$$

In cases 1 through 4, the sum of the indices of the four generators exceeds the bound $2n-2$, while in the fifth case equality is achieved. Since nontrivial generators always have positive index, this shows that the total number of generators must be ≤ 4 with equality only if all four are of type T_2. This gives us our bound when n is odd.

Next we examine the situation when n is even. We again show that there cannot be more than four generators, although with significantly more casework. We begin by assuming there are at least four generators and dealing with the cases where there is more than one T_1 element among these four:

Case 1:

$$4\mathrm{ind}(T_1) \ge 2n > 2n-2.$$

Case 2:

$$3\mathrm{ind}(T_1)+\mathrm{ind}(T_{2b}) \ge \frac{3n}{2}+\frac{n}{2}-1 = 2n-1 > 2n-2.$$

Case 3:

$$2\mathrm{ind}(T_1)+2\mathrm{ind}(T_{2b}) \ge n+(n-2) = 2n-2.$$

Since $\mathrm{ind}(T_{2a}) = \frac{n}{2} > \frac{n}{2}-1 = \mathrm{ind}(T_{2b})$, we can replace any of the type T_{2b} elements by type T_{2a} elements and the corresponding sum of indices will still exceed the bound $2n-2$. This means that if we have at least two type T_1 elements in our generating set of four elements, any choice of the other two elements will exceed or equal the bound $2n-2$.

Next we look at the cases where there is exactly one type T_1 element in our generating set:

Case 4:

$$\mathrm{ind}(T_1)+\mathrm{ind}(T_{2a})+2\mathrm{ind}(T_{2b}) \ge \frac{n}{2}+\frac{n}{2}+2\left(\frac{n}{2}-1\right) = 2n-2.$$

Case 5:

$$\mathrm{ind}(T_1)+3\mathrm{ind}(T_{2b}) \ge \frac{n}{2}+3\left(\frac{n}{2}-1\right) = 2n-3.$$

For the same reason as above, the equality achieved in case 4 allows us to ignore the cases where more than one type T_{2a} element appears. On the other hand, we do not exceed or meet the $2n-2$ bound in case 5. Fortunately, it is easy to show that we cannot add any element to this generating set. If we added a type T_{2a} element, we would reduce to case 4 with an added T_{2b} term and thus exceed the $2n-2$ bound. Suppose instead we added a type T_{2b} element, and thus obtaining

$$\mathrm{ind}(T_1) + 4\mathrm{ind}(T_{2b}) \geq \frac{n}{2} + 2n - 4 = 2n - 2 + \frac{n}{2} - 2.$$

Since n is even, we have $n \geq 4$, and so $\mathrm{ind}(T_1) + 4\mathrm{ind}(T_{2b}) \geq 2n-2$. If this inequality were strict we would be done, so we assume that in fact $\mathrm{ind}(T_1) + 4\mathrm{ind}(T_{2b}) = 2n-2$. This implies that $\frac{n}{2} - 2 = 0$, and so $n = 4$. Hence $\mathrm{ind}(T_{2b}) = 1$, and simple algebraic manipulation shows that $\mathrm{ind}(T_1) = 2$. The only element of index 2 in D_8 is r^2, so our generating set contains r^2 and four elements of type T_{2b}. Without loss of generality, let the element s be of type T_{2b}. Then if we write each of these elements in the form $r^{\alpha_i}s$, each of the α_i will be of even parity. Hence among r^2 and these four elements, every possible product will be be of the form $r^j s^k$ where j is even. Clearly this does not describe all of D_8, so this is not a valid generating set.

Finally, we deal with the cases of four elements of which none are of type T_1:

Case 6:

$$2\mathrm{ind}(T_{2a}) + 2\mathrm{ind}(T_{2b}) = n + 2\left(\frac{n}{2} - 1\right) = 2n - 2$$

Case 7:

$$\mathrm{ind}(T_{2a}) + 3\mathrm{ind}(T_{2b}) = \frac{n}{2} + 3\left(\frac{n}{2} - 1\right) = 2n - 3.$$

As before, the inequality $\mathrm{ind}(T_{2a}) > \mathrm{ind}(T_{2b})$ together with case 6 allows us to ignore cases where more than two of the elements are of type T_{2a}. As for case 7, observe that the only possible element can be of type T_{2b} and of of index 1. If this were the case, we would have a five element generating set of which one is of type T_{2a} and four of type T_{2b}. Without loss of generality, write the type T_{2a} as rs. This means the type T_{2b} elements are all of the form $r^j s$ where j is even. But then the product of all four of these elements is of this form as well, and so cannot have rs as its inverse. Since the product of these five elements is not equal to the identity, and since no more elements can be added without breaking the $2n-2$ bound, it follows that we cannot have five such elements in our generating set.

The remaining case is when all elements are of type T_{2b}. No numerical inequality is necessary here, because such a set can never generate D_{2n}. The reasoning is similar as in case 5 given above.

We have shown that if $x_1, ..., x_m$ satisfy conditions (i) - (iii), then $m = 3$ or $m = 4$. Given this information, we can prove our classification of sets of elements of this form.

We first deal with the case where n is odd. The index calculations show that the number of nontrivial generators must be equal to three or four, and can only be four when all are of type T_2. So we first assume there are 3 generators, denoted x_1, x_2, x_3. Now, since rotation elements alone cannot generate the dihedral group, at least one of these elements, say x_1, must be of the form $x_1 = r^k s$ for some k. Furthermore, the condition $x_1x_2x_3 = 1$ gives us

$$x_2x_3 = x_1^{-1} = x_1 = r^k s.$$

Now, if both x_2 and x_3 were of type T_2, we would have $x_2x_3 = (r^j s)(r^i s) = r^{j-i}$ for some i, j, and so cannot be equal to x_1. Hence at last one of these two, say x_2, is of type T_1. Then we have $x_2 = r^j$ for some j, and it follows that $x_3 = r^{k-j}s$. Since $\mathrm{ind}(x_1) + \mathrm{ind}(x_3) = n - 1$, we must have $\mathrm{ind}(x_2) = n - 1$. This implies that $\mathrm{orb}(x_2) = 1$, and so x_2 generates the subgroup $\langle r \rangle$. This occurs if and only if $(j, n) = 1$.

We have shown that any set of three elements satisfying the given conditions must be of the form $r^k s, r^j, r^{k-j}s$ where $(j, n) = 1$. It is easily seen that conversely, any three elements of this form will satisfy the given conditions. Hence in the case of n odd and three generators, we have classified all valid generating sets.

Again assuming that n is odd, we consider the case of four generators. Our index calculations showed that all four elements must be of type T_2. Denote these elements by x_1, x_2, x_3, x_4, and write $x_j = r^{\alpha_j}s$. Now, some product of these x_i must generate the rotation subgroup $\langle r\rangle$. The product of an odd number of x_j will not belong to this subgroup, and the product g of an even number of them will be of the form

$$g = (r^{t_1}s)(r^{s_1}s)\cdots(r^{t_m}s)(r^{s_m}s) = r^{(t_1-s_1)+(t_2-s_2)+\cdots+(t_m-s_m)}$$

where $m \in \mathbb{N}$ and each $t_i, s_i \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. Since some such product g generates $\langle r\rangle$, we must have

$$\sum_{i=1}^{m}(t_i - s_i) \equiv 1 \mod n,$$

which occurs if and only if the greatest common divisor of the differences of the α_j and n is equal to 1.

Furthermore, since we have

$$1 = (r^{\alpha_1}s)(r^{\alpha_2}s)(r^{\alpha_3}s)(r^{\alpha_4}s) = r^{(\alpha_1-\alpha_2)+(\alpha_3-\alpha_4)}$$

it follows that $\alpha_1 - \alpha_2 \equiv \alpha_4 - \alpha_3 \mod n$. This proves our claim when n is odd and all generators are of type T_2.

Next we look at the case where n is even. Again, our index calculations show that there are either three or four nontrivial generators in a valid generating set. We start by classifying three element generating sets. For the same reason as in the n odd case, such a set must contain at least one type $\mathrm{ind}(T_1)$ element and one type T_{2x} ($x \in \{a, b\}$) element. So the three possibilities are

1. $T_1 + 2T_{2a}$
2. $T_1 + T_{2a} + T_{2b}$
3. $T_1 + 2T_{2b}$.

We claim that the second possibility is the only valid one. For the first possibility we have

$$\mathrm{ind}(T_1) + 2\mathrm{ind}(T_{2a}) = (n - d) + 2\left(\frac{n}{2}\right) = 2n - d,$$

which implies that $d = 2$. Writing the type $\mathrm{ind}(T_{2a})$ elements as $r^i s$, $r^j s$, since both are of type $\mathrm{ind}(T_{2a})$ it follows that i and j must have the same parity. Hence there product will be of the form r^{i-j} where $i - j$ is even. Since $d = 2$ and n is even, this means that $r^j s$, $r^i s$, and the type $\mathrm{ind}(T_1)$ element cannot generate the subgroup $\langle r\rangle$, and so cannot generate D_{2n}. This eliminates the first possibility.

For the third possibility, we have

$$\mathrm{ind}(T_1) + 2\mathrm{ind}(T_{2b}) = (n - d) + 2\left(\frac{n}{2} - 1\right) = 2n - 2 - d,$$

which implies that $d = 0$, which is impossible. This eliminates the third the third possibility, and shows that if we have a three element generating set, we must have one element of each type. Observe that

$$\mathrm{ind}(T_1) + \mathrm{ind}(T_{2a}) + \mathrm{ind}(T_{2b}) = (n - d) + \left(\frac{n}{2}\right) + \left(\frac{n}{2} - 1\right) = 2n - 1 - d,$$

which implies that $d = 1$. In other words, the type $\operatorname{ind}(T_1)$ element is of the form r^k where $(k, n) = 1$. The condition $x_1x_2x_3 = 1$ implies that the first two elements are of the form $x_1 = r^i s$, $x_2 = r^j s$ where $j - i = k$. Note that since the $\operatorname{ind}(T_1)$ element alone generates $\langle r\rangle$, we automatically have these three elements satisfying $D_{2n} = \langle x_1, x_2, x_3\rangle$.

This shows that x_1, x_2, x_3 is a valid generating set for n even if and only if they are of the form

$$x_1 = r^i s, x_2 = r^j s, x_3 = r^k$$

where $i = j - k$, $(k, n) = 1$.

We now look at four element generating sets. Our index calculations gives three possibilities for valid generating sets:

1. $2\operatorname{ind}(T_1) + 2\operatorname{ind}(T_{2b})$
2. $\operatorname{ind}(T_1) + \operatorname{ind}(T_{2a}) + 2\operatorname{ind}(T_{2b})$
3. $2\operatorname{ind}(T_{2a}) + 2\operatorname{ind}(T_{2b})$.

We begin by eliminating the first possibility. Suppose we have x_1, x_2 of type $\operatorname{ind}(T_1)$ and x_3, x_4 of type $\operatorname{ind}(T_{2b})$ in our generating set. Then the equality

$$2n - 2 = (n - d_1) + (n - d_2) + 2\left(\frac{n}{2} - 1\right) = 2n - 2 + n - (d_1 + d_2)$$

gives us $d_1 + d_2 = n$. Since d_1 and d_2 are proper divisors of n, it follows that both must be equal to $\frac{n}{2}$. Hence $x_1 = x_2 = r^{\frac{n}{2}}$. But this means that $x_1x_2 = 1$, and so $1 = x_1x_2x_3x_4 = x_3x_4$, which means that $x_3 = x_4$ since both are of type $\operatorname{ind}(T_{2b})$. So if this were a valid generating set, we would have $D_{2n} = \langle x_1, x_3\rangle$ where $x_1 = r^{\frac{n}{2}}$ and $x_3 = r^k s$ for some k. But observe that x_1 commutes with x_3, and also that x_1 and x_3 are both of order 2. This means that $\langle x_1, x_3\rangle$ contains only four elements, which is impossible for the dihedral group. Hence we cannot have two type $\operatorname{ind}(T_1)$ and two type $\operatorname{ind}(T_{2b})$ elements.

The second possibility is not valid for a simple reason: Observe that the product of three elements of the form $r^k s$ will also be of this form, and so the product of a type $\operatorname{ind}(T_{2a})$ and two type $\operatorname{ind}(T_{2b})$ elements cannot have a type $\operatorname{ind}(T_1)$ element as its inverse. Hence we cannot have $x_1x_2x_3x_4 = 1$ in this case.

This leaves the third possibility. This can indeed lead to a valid generating set. By the same reasoning as in the n odd case, since sum product of the generators equals r we must have

$$\sum_{i=1}^{m}(t_i - s_i) \equiv 1 \mod n,$$

where $\{t_i - s_i\}$ is the set of nonzero differences of the exponents α_j for $x_j = r^{\alpha_j}s$. Since $\langle x_1, x_2, x_3, x_4\rangle$ contaings $\langle r\rangle$ and a type T_{2x} element, any such set will generate D_{2n}. This completes the classification of valid generating sets for D_{2n}.

3. The decomposition of $f(x)$

We now arrive at the core part of the paper. Recall that our aim is to describe an extension of the form $k(x)/k(h(x))$, motivated by the question of the shape of $h(x)$.

3.1. Ramification in $k(x)/k(t)$.

Theorem 3.1. *Let $f(x) = t$ be a degree-n rational function with monodromy group D_{2n}. Then $k(x)/k(t)$ has either three or four branch points, denoted $p_1, ...p_m$ (so that $m = 3$ or $m = 4$). The possible ramification types of these points are described as follows:*

1. *n is odd and $m = 3$: p_1 is totally ramified. p_2 and p_3 both have $\frac{n-1}{2}$ places lying above them with ramification index 2, and one place lying above them with ramification index 1.*
2. *n is odd and $m = 4$: Each p_i has $\frac{n-1}{2}$ places lying above them with ramification index 2, and one place lying above them with ramification index 1.*
3. *n is even and $m = 3$: p_1 is totally ramified. p_2 has $\frac{n}{2}$ places lying above it with ramification index 2. p_3 has $\frac{n}{2} - 1$ places lying above it with ramification index 2, and 2 places lying above it with ramification index 1.*
4. *n even and $m = 4$: p_1, p_2 have $\frac{n}{2}$ places lying above them with ramification index 2. p_3, p_4 have $\frac{n}{2} - 1$ places lying above it with ramification index 2, and 2 places lying above it with ramification index 1.*

Proof:

Let $L = k(x, y)$. By the Riemann Existence Theorem, there is a finite Galois extension of $k(x)$ whose Galois closure has Galois group D_{2n} and branch points $p_1, ..., p_k$ if and only if there exist generators $g_1, ..., g_k$ of D_{2n} such that $g_1 \cdots g_k = 1$ and each g_i has cycle structure describing to the ramification of the corresponding branch point p_i. Specifically, for each $1 \leq i \leq k$, the number of disjoint cycles of g_i corresponds to the number of preimages of p_i and the length of those cycles corresponds to the multiplicity of that preimage. This leads us to consider all possible generating sets of D_{2n} whose product is 1.

In addition, we have another restriction on possible generating sets of $D_{2n} = \mathrm{Gal}(L/k(t))$. Note that both $k(x)$ and $k(t)$ have genus 0 (see Theorem 3.2). The Riemann-Hurwitz Formula gives the following relation between the genus $g_{k(x)}$ of $k(x)$ and the genus $g_{k(t)}$ of $k(t)$:

$$2g_{k(x)} - 2 = n(2g_{k(t)} - 2) + \sum_{q \in Q} (e_q - 1),$$

where Q is the set of ramification points of $k(x)/k(t)$. Since $g_{k(x)} = g_{k(t)} = 0$, this gives the relation

$$2n - 2 = \sum_{q \in Q} (e_q - 1).$$

For each branch point p_i, let Q_i denote the set of places of $k(x)$ lying above p_i. By the Fundamental Equality, we have

$$\sum_{q \in Q_i} e(q|p_i) f(q|p_i) = n.$$

Since k is algebraically closed, each $f(q|p_i) = 1$, and so $\sum e_q = n$. The number of distinct places is of course equal to $|Q|$, which by the the Riemann Existence Theorem is equal to the number of orbits $\#(g_i)$ of $g_i \in D_{2n}$. Hence for each p_i we have

$$\sum_{q \in Q_i} (e_q - 1) = n - \#(g_i) = \mathrm{ind}(g_i),$$

and it follows that

$$\sum_{q\in Q}(e_q-1)=\sum_{i=1}^{k}\operatorname{ind}(g_i).$$

This reduces the problem of determining possible branch points of $k(x)/k(t)$ and their ramification types to the problem of finding generating sets $\{g_i\}$ of D_{2n} with trivial product and $\sum\operatorname{ind}(g_i)=2n-2$. This was solved completely in Lemma 2.6.

The rest of the proof is a mostly straightforward consequence of the Riemann Existence Theorem. Since the number of branch points corresponds to the number of generators of D_{2n} under the constraints given in Lemma 2.6, there are either 3 or 4 branch points. First suppose that there are 3 branch points, so that the generating set of D_{2n} is of the form

$$r^k s, r^j, r^{k-j}s$$

with $(j,n)=1$. If n is odd, then $r^k s$ and $r^{k-j}s$ both have cycle types consisting of $\frac{n-1}{2}$ 2-cycles and 1 1-cycle. $(j,n)=1$ implies that r^j generates the rotation subgroup of D_{2n}, and so is an n-cycle. This corresponds to the ramification type described in case 1.

If n is even, then since $(j,n)=1$ j is odd. Hence if k is even then $k-j$ is odd, and if k is odd then $j-k$ is even. In other words, the parity of k and $k-j$ must be different. We can choose the element $s\in D_{2n}$ to be the "flip" element (in the language of Lemma 2.6 above) that fixes no vertex of the regular n-gon. This means that all elements of D_{2n} of the form $r^i s$ with i even fix no vertex, and all elements of the form $r^i s$ with i odd fix exactly two vertices. Hence k and $k-j$ having different parities means that one consists of all 2-cycles and the other consists of $\frac{n}{2}-1$ 2-cycles and 2 1-cycles. Together with the n-cycle r^j, this yields the ramification type described in case 3.

Now suppose there are 4 branch points, so that D_{2n} has a generating set of the type

$$r^{\alpha_1}s, r^{\alpha_2}s, r^{\alpha_3}s, r^{\alpha_4}s,$$

with $\alpha_1-\alpha_2=\alpha_4-\alpha_3$, and $(t_1-s_1,...,t_l-s_l,n)=1$ where $\{t_i-s_i|1\le i\le l\}$ is the set of all differences for $t_i,s_i\in\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$, $t_i\neq s_i$. If n is odd then all four elements have the same cycle structure (described above), and thus has ramification type described in case 2. Suppose instead that n were even. Then since the set of differences of $\alpha_i-\alpha_j$ is coprime to n, they cannot all be even. Hence there is some $1\le i,j\le 4$ such that α_i and α_j have different parities. Without loss of generality, let $\alpha_1\not\equiv\alpha_2 \mod 2$. Then since $\alpha_1-\alpha_2=\alpha_4-\alpha_3$, α_3 and α_4 have differing parities as well. By the same reasoning as in the $m=3$, n even case, this means there are two elements in the generating set consisting of all 2-cycle, and two elements consisting of $\frac{n}{2}-1$ 2-cycles and 2 1-cycles. This corresponds to the ramification type described in case 4.

3.2. **The genus of L.**

Theorem 1.3 states that if $f^*(X,Y)$ has a quadratic irreducible factor, then f factors through some function h composed with a linear fractional. Furthermore, h must either be a Chebychev polynomial or a sub-Lattes map. A natural question to ask is precisely when each of these cases occur. As we shall eventually see, the answer lies in the genus of the Galois closure of $k(x)/k(h(x))$. Given the results of the previous section, this motivates us to ask how the ramification of an extension $k(x)/k(t)$ determines the genus of its Galois closure L.

We begin with a pair of basic lemmas which will be used in the proofs of the main theorems of this section.

Lemma 3.2. [5] *Let F be a function field over K, where K is either finite or algebraically closed. Then F has genus* 0 *if and only if F is rational.*

Lemma 3.3. [5] *Let E/F be an extension of function fields, let L be the Galois closure of E/F, and let p be a place of F. If p is unramified in E/F then p is unramified in L/F.*

Theorem 3.4. *Let $k(x)/k(t)$ be a degree-n extension with monodromy group D_{2n} and Galois closure L. If $k(x)/k(t)$ has three branch points, then L has genus 0 and is equal to $k(z)$ for some $z \in k(x, y)$.*

Proof:

Since L is a finite separable extension of $k(x)$, we can write $L = k(x, y)$ for some $y \in L$. Note that $\mathrm{Gal}(L/k(x))$ is not normal in $\mathrm{Gal}(L/k(t))$ (since subgroups generated by elements of the form $r^i s$ are not normal in D_{2n}). By Lemma 3.3, this means that any place p of $k(t)$ which is unramified in $k(x)$ is also unramified in L. By the multiplicativity of ramification in towers, any place p' of $k(x)$ lying over p must also be unramified in L. This shows that the only possible ramified places of $k(x)$ are those which lie over a place of $k(t)$ which is ramified in L. By the Riemann Existence Theorem there are three such places.

We first consider the infinite place p_∞ of $k(t)$, which we take to be the place with ramification index n in $k(x)$. Since $k(x)$ and $k(y)$ are $k(t)$-isomorphic, there exists $\sigma \in \mathrm{Gal}(L/k(t))$ such that $k(x)^\sigma = k(y)$. If g_1, g_2, g_3 are the elements of D_{2n} corresponding to branch points of $k(x)/k(t)$, then $g_1^\sigma, g_2^\sigma, g_3^\sigma$ are the elements corresponding to branch points of $k(y)/k(t)$. Furthermore, if p is a place of $k(x)$ lying over a place p' of $k(t)$, then p^σ is a place of $k(y)$ lying over p'. Therefore the ramification type of each place of $k(t)$ is invariant under σ. In particular, since p_∞ is totally ramified in $k(x)$, p_∞ is totally ramified in $k(y)$ as well.

Now let p be a place of L lying above p_∞. Then $p \cap k(x)$ and $p \cap k(y)$ are places in their respective fields which lie above p_∞, and hence both have ramification index n. Under the assumption that $(n, \mathrm{char}(k)) = 1$, applying Abhyankar's Lemma shows that $e(p/p_\infty) = n$. By the multiplicativity of ramification in towers, it follows that $p \cap k(x)$ is unramified in L. It follows that any place of $k(x)$ lying above p_∞ is unramified in L.

Since places in $k(x)$ lying above p_∞ are unramified in L, the only possible places of $k(x)$ ramified in L are those which lie over the branch points in $k(t)$ corresponding to involutions. We first suppose that n is odd. Then both branch points have $\frac{n+1}{2}$ places of $k(x)$ lying above them, of which $\frac{n-1}{2}$ have index 2 and the remaining place has index 1.

Let p_α be one these branch points, and let p be a place of L lying over p_α. Choose a place p_β of $k(x)$ lying over p_α with $e(p_\beta|p_\alpha) = 2$. Then if p' extends p_β to L, by the multiplicity of ramification in towers $e(p'|p_\alpha) \geq 2$. $L/k(t)$ is Galois, so all places of L lying over p_α have the same ramification index, and thus $e(p|p_\alpha) \geq 2$ for all places p of L lying over p_α.

One the other hand, given a place p of L lying over p_α, set $p_1 = p \cap k(x)$ and $p_2 = p \cap k(y)$. Then by Abhyankar's lemma we have

$$e(p|p_\alpha) = \mathrm{lcm}(e(p_1|p_\alpha), e(p_2|p_\alpha)) \leq 2$$

since the ramification indices of all places of $k(x)$ and $k(y)$ lying over p_α are either 1 or 2. Combined with our previous inequality, this shows that the ramification index of every place of L lying over p_α is precisely 2.

Now, recall that since n is odd, there is precisely one place p_β of $k(x)$ lying over p_α with $e(p_\beta|p_\alpha) = 1$. By the multiplicativity of ramification in towers, this implies there is a single ramified place of L over p_β, with ramification index 2. A symmetric argument applies to the other branch point in $k(t)$, which gives us precisely two places of $k(x)$ ramified in L, each with ramification index 2. We in fact obtain the same result when n is even, except in this case both ramified places of $k(x)$ lie over the same branch point of $k(t)$. The argument is essentially the same, however.

We have shown that in general there are two places of $k(x)$ ramified in L, each with ramification index 2. This shows that

$$\sum_{q\in Q}(e_q - 1) = 2,$$

where Q is the set of places of $k(x)$ ramified in L. This implies that the genus of L is 0, because by Riemann-Hurwitz

$$2g_L - 2 = (2g_{k(x)} - 2)[L : k(x)] + \sum_{q\in Q}(e_q - 1).$$

Since the genus of $k(x)$ is zero and $[L : k(x)] = 2$, this is equivalent to

$$2g_L = -2 + \sum_{q\in Q}(e_q - 1),$$

which as we have just shown is equal to zero. Hence L is of genus 0. By Lemma 3.2.1, L is rational, and hence is generated over k by some $z \in L$. Hence we can write $k(x, y) = L = k(z)$.

Theorem 3.5. *Let $k(x)/k(t)$ be a degree-n extension with monodromy group D_{2n} and Galois closure L. If $k(x)/k(t)$ has four branch points, L has genus 1 and is the function field of an elliptic curve.*

Proof:

Since L is a finite separable extension of $k(x)$, we can write $L = k(x, y)$ for some $y \in L$. Furthermore, let $E = k(x)$, $E' = k(y)$, and $F = k(t)$. By Lemma 3.3, any place p of F which is unramified in E is also unramified in L. By the multiplicativity of ramification in towers, if a place q of E lies over a place p of F unramified in E, then q is unramified in L. Hence the only places of E which can be ramified in L are those lying over ramified places of E/F. By the Riemann Existence Theorem there are four such places.

Let q be a place of E ramified in L. Then q lies above a place p of F ramified in E. Hence q is ramified in L, so there exists a place r of L such that r lies above p and $e(r|p) > 1$. By Abhyankar's Lemma, we have

$$e(r|p) = \operatorname{lcm}(e(r \cap E|p), e(r \cap E'|p)).$$

Since the ramification index of a place of E lying above any place of F is always either 1 or 2, it follows that $e(r|p) = 1$ or $e(r|p) = 2$. By multiplicativity of ramification in towers, it follows that $e(r|q) = 1$ or $e(r|q) = 2$ for any place of L lying above q.

We can now calculate $\sum(e_r - 1)$, where the sum is taken over places lying above the ramified places of L/E. First suppose that n is odd. Then E/F has four ramified places $p_1, ..., p_4$. Each p_i has $\frac{n+1}{2}$ places of E lying above it, each consisting of $\frac{n-1}{2}$ places q with $e(q|p_i) = 2$ and one place q' with $e(q'|p_i) = 1$. For any place r of L lying above p_i, $e(r|p_i) \leq 2$, and by multiplicativity we have equality for at least one such r. Since L/F is Galois, each place r lying above p_i has the same ramification index, so in fact for every r in L lying above p_i we have $e(r|p_i) = 2$. So if r lies above q with $e(q|p_i) = 2$, then $e(r|q) = 1$, and if r lies above the unique q' with $e(q'|p_i) = 1$ then $e(r|q') = 2$. This shows that there is precisely one place of E lying above each p_i that is ramified in L, and that it's ramification index is 2. Since these are the only possible ramified places of L/E, it follows that $\sum(e_r - 1) = 4$.

Now let n be even. The argument is similar, except that we now have two places p_1, p_2 of F with $\frac{n}{2}$ places of E lying above them and two places p_3, p_4 with $\frac{n}{2} + 1$ places lying above them. Each place q of E lying above p_1 and p_2 has $e(q|p_i) = 2$, and so there are no places of E which lie above these p_i and are ramified in L. For p_3, p_4, $\frac{n}{2} - 1$ of the places q lying above them have $e(q|p_j) = 2$, and the other two places q' have $e(q'|p_j) = 1$. By a similar argument as in the n

odd case, these two q' each have a place r of L lying above them so that $e(r|q') = 2$. Since there are two such r for each q' and two such q' for each of p_3, p_4, we again have $\sum(e_r - 1) = 4$.

We now apply the Riemann-Hurwitz formula to compute the genus of L:

$$\begin{aligned} 2g_L - 2 &= 2(2g_E - 2) + \sum(e_r - 1) \\ &= -2(0 - 2) + 4 \\ &= 0 \end{aligned}$$

which shows that $g_L = 1$, as claimed. Since every function field of genus 1 is the function field of some elliptic curve E, this completes the proof.

3.3. **Proof of main theorem.**

This section collects several separate results which, when taken as a whole, form the proof of Theorem 1.3.

Lemma 3.6. *Let $q(X, Y) \in k[X, Y]$ be an absolutely irreducible factor of $f^*(X, Y)$ that is quadratic in both X and Y, and let x, y be transcendental over the field k such that $q(x, y) = 0$. Then the following hold:*

1. *$k(x) \cap k(y) = k(t)$ for some t transcendental over k.*
2. *$k(x, y)/k(t)$ is Galois.*
3. *Gal$(k(x, y)/k(t)) \cong D_{2n}$.*

Proof:

1. Since $q(x, y) = 0$, $f^*(x, y) = 0$, and so $f(x) = f(y)$. In particular $f(x) \in k(x) \cap k(y)$, and so $k(x) \cap k(y)$ is a subfield of $k(x)$ (and of $k(y)$ properly containing k. By Luroth's theorem, this means that $k(x) \cap k(y) = k(t)$ for some $t \in k(x) \cap k(y)$.

2. Viewing $q(x, y)$ as a polynomial in y over $k(x)$, we see that $k(x, y)$ is the splitting field of q over $k(x)$. Since char$(k) \neq 2$, it follows that $k(x, y)/k(x)$ is Galois of degree 2, as is $k(x, y)/k(y)$ by symmetry. Let $G = \text{Gal}(k(x, y)/k(t)$, $H = \text{Gal}(k(x, y)/k(x))$, and $K = \text{Gal}(k(x, y)/k(y))$. Since $H, K \leq G$, $\text{Fix}(G) \leq \text{Fix}(H)$ and $\text{Fix}(G) \leq \text{Fix}(K)$. Since $k(x, y)/k(x)$ and $k(x, y)/k(y)$ are both Galois, $\text{Fix}(H) = k(x)$ and $\text{Fix}(K) = k(y)$. Hence $\text{Fix}(G) \leq k(x) \cap k(y)$. Since by definition $k(x) \cap k(y) \leq \text{Fix}(G)$, it follows that $k(t) = k(x) \cap k(y) = \text{Fix}(G)$, and so $k(x, y)/k(t)$ is Galois.

3. Let G, H, and K be as before. Note that $|H| = |K| = 2$, and let $H = \langle\sigma\rangle$, $K = \langle\tau\rangle$. Since $k(x) \neq k(y)$, $H \neq K$, and in particular $\sigma \neq \tau$. We claim that $G = \langle\sigma, \tau\rangle$. Let $G_0 = \langle\sigma, \tau\rangle$, and consider $\text{Fix}(G_0)$. This field consists of all $\alpha \in k(x, y)$ such that $\sigma(\alpha) = \alpha$ and $\tau(\alpha) = \alpha$. But this is just $\text{Fix}(H) \cap \text{Fix}(K)$, or $k(x) \cap k(y) = k(t)$. Hence $\text{Fix}(G_0) = k(t) = \text{Fix}(G)$, and since $k(x, y)/k(t)$ is Galois it follows that $G = \langle\sigma, \tau\rangle$. Letting $n = |\sigma\tau|$, we then have the presentation

$$G = \langle\sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^n = 1\rangle,$$

which is that of the dihedral group of order n.

Remark 3.7. From this point forward we assume that $n > 2$. The $n = 2$ case shall be dealt with later.

Lemma 3.8. *$k(x)/k(t)$ has either three or four branch points, whose ramification types are equal to one of the four cases given in Theorem 3.1.*

Proof:

By Lemma 3.6, $k(x,y)/k(t)$ is Galois with Galois group D_{2n}. Under our assumption that $n > 2$, the involution that does not belong to the rotation subgroup generates a non-normal subgroup D_{2n}. Since $k(x)$ is the fixed field of this subgroup, the extension $k(x)/k(t)$ is not Galois. Letting $h : x \mapsto t$, we have $\mathrm{Mon}(h(x)) = D_{2n}$. Hence Theorem 3.1 applies to the extension $k(x)/k(t)$.

Theorem 3.9. *Suppose $k(x)/k(t)$ has three branch points. Then the following hold:*

(a) $f(x) = g \circ T_n \circ \mu_1(x)$ and $f(y) = g \circ T_n \circ \mu_2(y)$ for some rational function g and linear fractionals μ_1, μ_2.

(b) Let $q'(X,Y)$ denote the numerator of $q(\mu_1^{-1}(X), \mu_2^{-1}(Y))$. If n is odd, then $q'(X,Y)$ divides $T_n^*(X,Y)$ in $k[X,Y]$. If n is even, then $q'(X,Y)$ divides $T_n(X) + T_n(Y)$.

Proof:

(a) By Lemma 3.2, $k(x,y) = k(z_0)$ for some $z_0 \in k(x,y)$. Choose $\sigma \in \mathrm{Gal}(k(z_0)/k(t))$ such that $k(x) = \mathrm{Fix}(\langle\sigma\rangle)$. We first claim that there exists z such that $k(z) = k(z_0) = k(x,y)$ and the action of σ on z is given by $z \mapsto z^{-1}$. First note that $\mathrm{Gal}(k(z_0)/k) \cong PGL_2(k)$ (from here on we identify the two), and that the image of z_0 under any $T \in PGL_2(k)$ also generates $k(z_0)$ over k.

We claim that the set of elements of order 2 in $PGL_2(k)$ form a single conjugacy class. Let $\sim$ denote the conjugacy relation and let $M \in PGL_2(k)$ with $|M| = 2$. Viewing $PGL_2(k)$ as the quotient $GL_2(k)/Z(k^2)$, we can choose a representative matrix M_0 with the property $M_0 \notin Z(k^2)$ and $M_0^2 \in Z(k^2)$. Since k is algebraically closed, there exists $J_0 \in GL_2(k)$ where $M_0 \sim J_0$ and J_0 is in Jordan Canonical Form.

Letting J be the coset of $PGL_2(k)$ containing J_0, since $M_0 \sim J_0$ in $GL_2(k)$ clearly $M \sim J$ in $PGL_2(k)$. Hence $|J| = 2$. Concretely, this means that J_0 is not a scalar matrix but J_0^2 is a scalar matrix. Writing

$$J_0 = \begin{pmatrix} \lambda & 1 \\ 0 & \eta \end{pmatrix},$$

we see that

$$\begin{aligned} J_0^2 &= \begin{pmatrix} \lambda & 1 \\ 0 & \eta \end{pmatrix} \begin{pmatrix} \lambda & 1 \\ 0 & \eta \end{pmatrix} \\ &= \begin{pmatrix} \lambda^2 & \lambda + \eta \\ 0 & \eta^2 \end{pmatrix} \end{aligned}$$

which implies that $\lambda = -\eta$ since J_0^2 is a scalar matrix.

The above shows that every matrix of order 2 is conjugate to a matrix of the form

$$\begin{pmatrix} \lambda & 1 \\ 0 & -\lambda \end{pmatrix},$$

each of which is equivalent modulo the subgroup of scalar matrices $Z(k^2)$. Hence in $PGL_2(k)$, the elements of order 2 form a single conjugacy class.

Now, since $\sigma \in \mathrm{Gal}(k(z_0)/k(t)) \leq \mathrm{Gal}(k(z_0)/k) = PGL_2(k)$ we can view σ as an element of $PGL_2(k)$. In addition we know that $|\sigma| = 2$. Clearly the map $\tau : z_0 \mapsto \frac{1}{z_0}$ is also of order 2. By what we have just shown, these two elements of $PGL_2(k)$ are conjugate. Let $\ell \in PGL_2(k)$ such that $\sigma = \tau^\ell$ and let $z = \ell(z_0)$. Then

$$\sigma(z) = \sigma \circ \ell(z_0) = \ell \circ \tau(z_0) = \ell\left(\frac{1}{z_0}\right) = z^{-1}.$$

Since ℓ is a fractional linear transformation, $k(z) = k(z_0) = k(x, y)$.

We next claim that $k(x) = k(z + z^{-1})$. Write $u = z + z^{-1}$. Since $k(x) = \mathrm{Fix}(\langle\sigma\rangle)$ and clearly $\sigma(u) = u$, we have $k(u) \leq k(x)$. It is enough to show that $[k(z) : k(x)] = [k(z) : k(u)]$. Consider the following polynomial $p(X) \in k(u)[X]$:

$$p(X) = X^2 - uX + 1.$$

A simple derivation shows that z is a root of P:

$$\begin{aligned} P(z) &= z^2 - uz + 1 \\ &= z^2 - \left(z + z^{-1}\right) z + 1 \\ &= z^2 - z^2 - 1 + 1 = 0 \end{aligned}$$

Hence $[k(z) : k(u)] \leq 2$. Since $k(u)$ is a subfield of $k(x)$, clearly $[k(z) : k(u)] \geq [k(z) : k(x)] = 2$, and so we have equality throughout. This shows that $k(x) = k(z + z^{-1})$, as desired.

Our next goal is to show that $k(t) = k(z^n + z^{-n})$ by considering a generator θ of the rotation subgroup of D_{2n}. We claim that $\mathrm{Fix}(\langle\theta\rangle) = k(z^n)$. By a linear fractional change of t, we can assume that the infinite place of $k(x)$ lies above the infinite place of $k(t)$, and that this place is the unique totally ramified place of $k(x)/k(t)$. Since θ fixes t, it fixes the preimage set of ∞ under the map $z \mapsto t$. Since $k(x) = k(z + z^{-1})$, this means that θ fixes $\{0, \infty\}$. Hence $\theta : z \mapsto \alpha z^{\epsilon}$ for some $\alpha \in k$ and $\epsilon \in \{1, -1\}$.

Suppose θ maps $z \mapsto \alpha z^{-1}$. Then $k(z + z^{-\alpha})$ is fixed by θ. This implies that $[k(z) : \mathrm{Fix}(\langle\theta\rangle)] \leq 2$, contradicting the fact that $|\theta| = n > 2$. Hence $\theta(z) = \alpha z$ for some $\alpha \in k$. Moreover, it is clear that α must be a primitive n'th root of unity. This means that $k(z^n) \leq \mathrm{Fix}(\langle\theta\rangle)$, and since $[k(z) : k(z^n)] = n = |\theta| = [k(z) : \mathrm{Fix}(\langle\theta\rangle)]$, we in fact have equality.

The group D_{2n} is can always be generated by an n-cycle and an involution which is not a power of that n-cycle. Thus $\mathrm{Gal}(k(z)/k(t)) = \langle\sigma, \theta\rangle$. It follows that $k(t) = \mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\theta) = k(z + z^{-1}) \cap k(z^n)$, which can easily be verified to be equal to $k(z^n + z^{-n})$.

We can finally prove that f factors through a Chebychev composed with a linear fractional. Since $k(t) = k(z + z^{-1})$, there exists a rational function h such that $h(x) = z + z^{-1}$. Similarly, since $k(x) = k(z + z^{-1})$, there exists a linear fractional μ_1 such that $\mu_1(x) = z + z^{-1}$. Now, we have

$$h \circ \mu_1^{-1}(z + z^{-1}) = h(x) = z^n + z^{-n},$$

so that $h \circ \mu_1^{-1}$ satisfies the functional equation defining a Chebychev. Hence $h \circ \mu_1^{-1} = T_n$, and so $h = T_n \circ \mu_1$.

Now, since $f(x) = f(y)$, clearly $f(x) \in k(x) \cap k(y)$. $k(x) \cap k(y)$ is generated over k by $h(x)$, which means that $f(x) = g \circ h(x)$ for some rational function g. By what we have just shown, we obtain $f(x) = g \circ T_n \circ \mu_1(x)$.

We still need to examine the composition of $f(y)$. We claim that $k(y) = k(\alpha^j z + z^{-1})$. Let $\tau \in \mathrm{Gal}(k(z)/k(t)) \cong D_{2n}$ such that $k(y) = \mathrm{Fix}(\tau)$. Since $\mathrm{Gal}(k(z)/k(y))$ is a non-normal degree-2 subgroup of D_{2n}, we must have $\tau = \theta^j\sigma$ for some j. Clearly $k(\alpha^j z + z^{-1}) \leq \mathrm{Fix}(\tau)$. The argument that $[k(z) : k(\alpha^j z + z^{-1})] = 2$ is nearly identical to the one given above for $k(z) : k(z + z^{-1})$, which shows that $k(\alpha^j z + z^{-1}) = \mathrm{Fix}(\tau) = k(y)$.

Since $k(y) = k(\alpha^j z + z^{-1})$, there is a linear fractional μ_2 such that $\mu_2(y) = \alpha^j z + z^{-1}$. Since α is an n'th root of unity, we have $T_n(\alpha^j z + z^{-1}) = z^n + z^{-n}$, and so obtain

$$g \circ T_n \circ \mu_2(y) = g(z^n + z^{-n}) = g \circ T_n \circ \mu_1(x) = f(x) = f(y).$$

Thus $f(y) = g \circ T_n \circ \mu_2(y)$, as claimed.

(b) First suppose that n is odd. Identifying $\mathrm{Gal}(k(z)/k(t))$ with D_{2n}, we have $k(x) = \mathrm{Fix}(\langle s \rangle)$ for $s : z \mapsto z^{-1}$ and $k(y) = \mathrm{Fix}(\langle r^j s \rangle)$ for $r : z \mapsto \alpha z$, where α is a primitive n'th root of unity. Since n is odd, s and $r^k\ s$ have the same cycle structure, and thus are conjugate via some $\tau \in D_{2n}$ of the form $\tau : z \mapsto \alpha^k z$.

Let $x_0 = z + z^{-1}$ and $y_0 = \alpha^k z + \frac{1}{\alpha^k z}$. Then $k(x) = k(x_0)$, $k(y) = k(y_0)$, and $y_0 = \tau(x_0)$. So we have

$$T_n(x_0) = z^n + z^{-n} = (\alpha^k z)^n + \frac{1}{(\alpha^k z)^n} = T_n(\tau(x_0)) = T_n(y_0).$$

This shows that (x_0, y_0) is a solution of $T_n^*(X,Y) = T_n(X) - T_n(Y)$.

On the other hand, since $q(x,y) = 0$ and $q'(x_0, y_0)$ is defined as the numerator of

$$q(\mu_1^{-1}(x_0), \mu_2^{-1}(y_0)) = q(x,y),$$

it follows that (x_0, y_0) is a solution of $q'(X,Y)$ as well. Now, if q' were reducible, then since it is a quadratic we would have $x_0 = L(y_0)$ for some linear function L. But this would imply that $k(y) = k(y_0) = k(x_0) = k(x)$, a contradiction. Thus q' is irreducible.

Consider the polynomial $T_n^*(X, y_0) \in k(y)[X]$. $q'(X, y_0)$ is the minimal polynomial of x_0 over $k(y)$, and so $q'(X, y_0)$ divides $T_n^*(X, y_0)$ in $k(y)[X]$. Since $k(y) = k(y_0)$, we can thus write

$$T_n^*(X, y_0) = q'(X, y_0) h(X, y_0)$$

for some $h \in k(y_0)[X]$. By Gauss's lemma, since $T_n^*(X, y_0) \in k[y_0][X]$ factors over $k(y_0)$, it must also factor over $k[y_0][X]$. Moreover, since $q'(X, y_0)$ is a polynomial in y_0, this implies that $h(X, y_0)$ must be a polynomial in y_0 as well.

We have shown that $q'(X, y_0)$ divides $T_n^*(X, y_0)$ in the polynomial ring $k[y_0][X]$. But since $k[y_0] \equiv k[Y]$ via the isomorphism $y_0 \mapsto Y$, it follows that $q'(X,Y)$ divides $T_n^*(X,Y)$ in $k[X,Y]$.

Now let n be even, and consider $\mathrm{Gal}(k(z)/k(s))$ where $s = z^{2n} + z^{-2n}$. Let β be a primitive $2n$'th root of unity. Note that $\beta^2 = \alpha$. Letting $s, r_0 \in D_{4n}$ such that $s : z \mapsto z^{-1}$ and $r_0 : z \mapsto \beta z$, we see that $k(x) = \mathrm{Fix}(\langle s \rangle)$ and

$$k(y) = \mathrm{Fix}(\langle r^j s \rangle) = \mathrm{Fix}(\langle r_0^{2j} s \rangle),$$

since $r = r_0^2$ when D_{2n} is identified as a subgroup of D_{4n}. Since the cycle structure of the elements of the from $r_0^i s$ alternates depending on the parity of i, it follows that s and $r^j s$ have the same cycle structure in D_{4n}. Hence they are conjugate (in D_{4n}) via an automorphism of the form $\sigma : z \mapsto \beta^k z$.

Now, noting that $\beta^n = \alpha^{n/2}$, we see that $\beta^n = -1$. Hence

$$T_n(x_0) = z^n + z^{-n} = -\left(\beta^{kn} z^n + \frac{1}{\beta^{kn} z^n}\right) = -T_n(\sigma(x_0)) = -T_n(y_0).$$

This shows that (x_0, y_0) is a solution of $T_n(X) + T_n(Y)$. The remainder of the proof is identical to the n odd case.

Remark 3.10. The point of part (b) of Theorem 3.9 is to show that when $f^*(X,Y)$ has a quadratic factor, we can actually say more then just that f factors through $T_n \circ \mu$ - the quadratic factor is in a sense coming from the Chebychev polynomial in the first place.

Remark 3.11. It is worth noting that if $f(x)$ is a polynomial, then the positive characteristic version of Ritt's theorem can be used to show that in fact $\mu_1 = \mu_2$ in Theorem 3.9. We shall not prove this, however.

Theorem 3.12. *If $k(x)/k(t)$ has four branch points, then $f(x) = g \circ \Lambda \circ \mu(x)$ for some rational function g and linear fractional μ.*

Proof

Let τ be the element of $\mathrm{Gal}(L/k(t))$ such that $k(x) = \mathrm{Fix}(\langle\tau\rangle)$. Note that τ is an involution. For convenience, we identify τ with the rational map on E induced by τ. We claim that τ is of the form $\tau : P \mapsto \pm P + Q$ for some fixed Q in E. To see this, first note that

$$\mathrm{Aut}(L) = \mathrm{Aut}(K(E)) \cong \mathrm{Aut}(E) \ltimes \langle \sigma_Q \mid Q \in E\rangle,$$

where $\sigma_Q : P \mapsto P + Q$. Write $\tau = (\omega, \sigma) \in \mathrm{Aut}(E) \ltimes \langle\sigma_Q\rangle$. Then since τ is an involution, we have

$$(1, 1) = \tau^2 = (\omega^2, \sigma(\sigma^\omega)).$$

In particular this shows that ω either the identity or is the unique involution in $\mathrm{Aut}(E)$, namely the map $\omega : P \to -P$. Since $\sigma(\sigma^\omega) \in \langle\sigma_Q\rangle$, this proves our claim.

Now that we know the action of τ on our elliptic curve E, we want to choose a distinguished point $O \in E$ such that $\tau : P \to -P$ in the resulting group structure. To do so, we recall the bijection of abelian groups

$$E \cong \mathrm{Pic}^0(E),$$

where $\mathrm{Pic}^0(E)$ is the degree 0 part of the divisor class group of E. The bijection $\phi : E \to \mathrm{Pic}^0(E)$ maps $P \mapsto (P) - (W)$, where W is the distinguished point of E.

First suppose that $\tau : P \mapsto P + Q$ for some $Q \in E$ in the group given by the distinguished point W. We define a new group structure by choosing our new distinguished point O to be the unique point satisfying

$$2O = 2P + Q.$$

Note that since k is the algebraic closure of a finite field, the group structure on E is a divisible group. Hence such a point O indeed exists. Furthermore, since $\mathrm{char}k \neq 2, 3$, we have $(A+B) = (A) + (B)$ for all $A, B \in E$ (by [6], III.3.4-(e)), so $2(O) = 2(P) + (Q)$ as well.

Now, using the identity

$$(-P) = 2(O) - (P),$$

we have

$$\begin{aligned}\phi(-P) &= 2(O) - (P) - (O) \\ &= 2(P) + (Q) - (P) - (O) \\ &= (P) + (Q) - (O) \\ &= (P + Q) - (O) = \phi(P + Q).\end{aligned}$$

Since ϕ is a bijection this implies that $P + Q = -P$ on E. Hence $\tau : P \mapsto -P$ in the group structure induced by the distinguished point O. The proof in the case that $\tau : P \mapsto -P + Q$ is similar.

We have shown that given $\tau \in \mathrm{End}(E)$ of order 2, we can choose coordinates on E such that $\tau : P \mapsto -P$. Hence $\tau \in \mathrm{Aut}(E)$, and so $\Gamma = \langle\tau\rangle$ is a subgroup of $\mathrm{Aut}(E)$ of order 2. By ([7], Prop 6.37), the quotient curve E/Γ is isomorphic to $\mathbb{P}^1_k$.

Let $\sigma \in \mathrm{Aut}(K(E)) = L$ such that σ generates the rotation subgroup N of $D_{2n} = \mathrm{Gal}(L/k(t))$. σ must map $P \to P + R$ for some fixed $R \in E$, and so $\mathrm{Fix}(\sigma)$ corresponds to the quotient curve E/R, which we denote by E_0. Since N is normal in D_{2n}, $K(E_0)/k(t)$ is Galois with Galois group

$$\mathrm{Gal}(K(E_0)/k(t)) \cong \mathrm{Gal}(L/k(t))/N) = D_{2n}/\mathbb{Z}_n = \mathbb{Z}_2.$$

Now, viewing $D_{2n} = \langle \tau, \sigma \rangle$, we see that $\mathrm{Gal}(E_0/k(t)) = \langle \tau \mod N \rangle$. Denoting $\tau \mod N$ by $\bar{\tau}$, we see that for each $P_0 \in E_0$ we have $\bar{\tau} : P_0 \mapsto -P_0$.

Finally, since $\langle \bar{\tau} \rangle$ is a nontrivial subgroup of $\mathrm{Aut}(E_0)$, the corresponding quotient curve with function field $k(t)$ is isomorphic to $\mathbb{P}^1_k$. Hence we obtain the following commutative diagram:

$$\begin{tikzcd}
E \arrow[r, "\theta"] \arrow[d, "\pi_1"] & E_0 \arrow[d, "\pi_2"] \\
\mathbb{P}^1_k \arrow[r, "\Lambda"] & \mathbb{P}^1_k
\end{tikzcd}$$

Here π_1, π_2 are the natural projection maps and θ is an isogeny. By ([7], 6.4), Λ is a sub-Lattes map.

The above shows that $k(t) = k(\Lambda(x))$, and since $f(x) \in k(t)$ we have $f(x) = g \circ \Lambda \circ \ell(x)$ for some linear fractional ℓ. Hence f factors through a sub-Lattes map up to a linear fractional.

Theorem 3.13. *In the setup of Lemma 3.6, suppose that $n = 2$. Then $f(x)$ factors through $T_2 \circ \mu$ for some linear fractional μ.*

Proof:

Applying Riemann-Hurwitz to the extension $[k(x) : k(t)]$ yields

$$2g_{k(x)} - 2 = n(2g_{k(t)} - 2) + \sum (e_p - 1),$$

which implies that $\sum(e_p - 1) = 2$ since $n = 2$ and $g_{k(x)} = g_{k(t)} = 0$. Since $1 \leq e_p \leq n = 2$ for each place of $k(x)$, it follows that $h(x)$ has two branch points, each of which are totally ramified with ramification index 2. This is the same ramification structure of T_2, so they are equivalent up to a linear fractional. Since $f(x) \in k(t)$, the theorem follows.

Theorem 3.14. *Let h be a degree-n rational function with monodromy group D_{2n}. If $f(x) = u \circ h \circ \mu(x)$ for some rational function u and linear fractional μ, then $f^*(X, Y)$ has a quadratic irreducible factor.*

Proof:

Write $g(x) = h\mu_1$ and let L be the Galois closure of $k(x)/k(g(x))$. Since $[k(x) : k(g(x))] = n$ and $[L : k(g(x))] = 2n$, clearly $[L : k(x)] = 2$.So if we let y be a primitive element for $L/k(x)$ and q be the minimal polynomial of y over $k(x)$, then $\deg(q) = 2$. In addition, since $f^*(x, Y)$ is polynomial in $k(x)[Y]$ with y as a root, it follows that $q(Y)|f^*(x, Y)$.

Now, we cannot have $q(Y) \in k[Y]$, since that would imply that y is algebraic over k. Furthermore, we can show that in fact $q(Y) \in k[x, Y]$. $k[x]$ is a UFD, so Gauss's Lemma applies. Hence $f^*(x, Y)$ factors over $k[x]$ into irreducible factors of the same Y-degree as their corresponding factors over $k(x)$. Hence $q(Y)$ can be taken to lie in $k[x]$.

The above shows that we can write $q(x, Y) = q(Y)$ and view it as a polynomial in two variables such that $q(x, y) = 0$. Hence x is a root of the polynomial $q(X, y) \in k[y][X]$. We claim $q(X, y)$ is irreducible over $k(y)$. Suppose not. Then again by Gauss's Lemma we would have $q(X, y)$ factoring over $k[y]$. Since the y-degree of $q(X, y)$ is 2, this would imply that the factors are of the form $P(X) - y$, where P is a polynomial. Hence $y = P(x)$, and so $y \in k(x)$. This contradicts the fact that $[L : k(x)] = 2$, so $q(X, y)$ is irreducible over $k(y)$.

We next show that $[L : k(y)] = 2$. Since $q(x, y) = 0$ and $q(X, Y)$ is a factor of $f^*(X, Y)$, we have $f(x) = f(y)$. Hence $k(f(x)) = k(f(y))$, and so we obtain the formula

$$[L : k(x)][k(x) : k(f(x))] = [L : k(f(x))] = [L : k(y)][k(y) : k(f(y)].$$

Clearly $[k(x) : k(f(x))] = [k(y) : k(f(y))]$, so we have $[L : k(y)] = [L : k(x)] = 2$, as desired.

Since x generates L over $k(y)$, this derivation shows that the minimal polynomial of x over $k(y)$ has degree 2. Since $q(X, y)$ is irreducible and has x as a root, it follows that $q(X, y)$ has X-degree 2. Hence $q(X, Y)$ is quadratic in both variables, absolutely irreducible, and satisfies $q(x, y) = 0$. The last condition implies that $q(X, Y)|f^*(X, Y)$, so this completes the proof.

Corollary 3.15. *Let T_n denote the n'th Chebychev polynomial and Λ a degree n sub-Lattes map. If $f(x) = u \circ T_n \circ \mu_1$ or $f(x) = w \circ \Lambda \circ \mu_2$ for some rational functions u, w and linear fractionals μ_1, μ_2, then $f^*(X, Y)$ has a quadratic irreducible factor.*

First suppose that $n > 2$. Then T_n has ramification type corresponding to the cycle structure given in case (1) of Lemma 2.6. Similarly, Λ has ramification type corresponding to case (2) of Lemma 2.6. By the Riemann Existence Theorem both T_n and Λ have monodromy group D_{2n}, and so applying Theorem 3.14 gives the desired result.

Now let $n = 2$. Write $f(x) = u \circ h(x) \circ \mu$ $h(x) = T_n$ or $h(x) = \Lambda$. Writing $t = h(x)$, by hypothesis we have $[k(x) : k(h(x))] = 2$. So by a similar argument as in Theorem 3.13 we see that $h(x)$ is equivalent to T_2. Hence we can write $f(x) = v \circ T_n \circ \omega$ for some rational function v and linear fractional ω. In other words, $f(x)$ factors through T_2 up to a linear fractional. The fact that $f^*(X, Y)$ has a quadratic irreducible factor in this case can be verified via computation.

Remark 3.16. When f is known to factor through $T_n \circ \mu$, the above proof is not really necessary. The irreducible quadratic factors of T_n^* are known, and from this it is not hard to compute $(T_n \circ \mu)^*$. However Theorem 3.14 has the advantage of taking care of both the Chebychev case and the sub-Lattes map case at once.

Acknowledgments

I would like to thank my advisor Danny Neftin for his help, support, and guidance throughout this project. I would also like to thank Michael Zieve, who suggested the original problem and the approach we used to solve it. Finally, I would like to thank the University of Michigan Mathematics REU program and the NSF for making this project possible.

References

[1] M. T. Acosta, J. Gomez-Calderon, The second-order factorable core of polynomials over finite fields.

[2] J. Gomez-Calderon, The third-order factorable core of polynomials over finite fields.

[3] J. Gomez-Calderon, D. Madden, Polynomials with small value sets over finite fields.

[4] R. Nevanlinna, Einige Eindeutigkeitss?atze in der Theorie der Meromorphen Funktionen.

[5] H. Stichtenoth , Algebraic Function Fields and Codes.

[6] J. Silverman, The Arithmetic of Elliptic Curves.

[7] J. Silverman, The Arithmetic of Dynamical Systems.

[8] P. Muller, M. Zieve , On Ritt's Polynomial Decomposition Theorems.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA
E-mail address: levieric@umich.edu