Algebra & Number Theory

Volume 13
2019
No. 4

A finiteness theorem for specializations of dynatomic polynomials

David Krumm

msp

msp

ALGEBRA AND NUMBER THEORY 13:4 (2019)
dx.doi.org/10.2140/ant.2019.13.963

A finiteness theorem for specializations of dynatomic polynomials

David Krumm

Let t and x be indeterminates, let $\phi(x) = x^2 + t \in \mathbb{Q}(t)[x]$, and for every positive integer n let $\Phi_n(t, x)$ denote the n-th dynatomic polynomial of ϕ. Let G_n be the Galois group of Φ_n over the function field $\mathbb{Q}(t)$, and for $c \in \mathbb{Q}$ let $G_{n,c}$ be the Galois group of the specialized polynomial $\Phi_n(c, x)$. It follows from Hilbert's irreducibility theorem that for fixed n we have $G_n \cong G_{n,c}$ for every c outside a thin set $E_n \subset \mathbb{Q}$. By earlier work of Morton (for $n = 3$) and the present author (for $n = 4$), it is known that E_n is infinite if $n \leq 4$. In contrast, we show here that E_n is finite if $n \in \{5, 6, 7, 9\}$. As an application of this result we show that, for these values of n, the following holds with at most finitely many exceptions: for every $c \in \mathbb{Q}$, more than 81% of prime numbers p have the property that the polynomial $x^2 + c$ does not have a point of period n in the p-adic field $\mathbb{Q}_p$.

1. Introduction

Let c be a rational number and let $\phi_c(x) = x^2 + c$. Given any algebraic number x_0, we may consider the sequence $x_0, \phi_c(x_0), \phi_c(\phi_c(x_0)), \ldots$. If this sequence is periodic with period n, we say that x_0 has period n under iteration of ϕ_c. By allowing c and x_0 to vary in $\mathbb{Q}$, one can find examples where x_0 has period 1, 2, or 3 under ϕ_c. For instance, the pairs

$$(c, x_0) = (0, 0),\ (-1, 0),\ \left(\tfrac{-29}{16}, \tfrac{5}{4}\right)$$

provide examples of periods 1, 2, and 3, respectively.

Poonen [1998] conjectured that if $n > 3$, then there does not exist $c \in \mathbb{Q}$ such that the polynomial ϕ_c has a rational point of period n. This has been proved for periods 4 and 5, and also for period 6 assuming the Birch–Swinnerton-Dyer conjecture; see [Morton 1998; Flynn et al. 1997; Stoll 2008]. The present paper is concerned with a strong form of Poonen's conjecture which was stated by the author in [Krumm 2016]: if $n > 3$, then for every $c \in \mathbb{Q}$ there exist infinitely many primes p such that ϕ_c does not have a point of period n in the p-adic field $\mathbb{Q}_p$. In fact, we will consider here a further strengthening of Poonen's conjecture.

Conjecture 1.1. *Fix $n > 3$. For every $c \in \mathbb{Q}$, let $T_{n,c}$ denote the set of primes p such that ϕ_c does not have a point of period n in $\mathbb{Q}_p$, and let $\delta(T_{n,c})$ be the Dirichlet density of $T_{n,c}$. Then $\delta(T_{n,c}) > 0$ for all $c \in \mathbb{Q}$.*

MSC2010: primary 37P05; secondary 11S15, 37P35.
Keywords: arithmetic dynamics, function fields, Galois theory.

In order to study these conjectures it is useful to consider a family of *dynatomic polynomials* defined as follows. For every positive integer n we define a two-variable polynomial $\Phi_n \in \mathbb{Q}[t, x]$ by the formula

$$\Phi_n(t, x) = \prod_{d \mid n} (\phi^d(x) - x)^{\mu(n/d)}, \tag{1-1}$$

where μ is the Möbius function, $\phi(x) = x^2 + t \in \mathbb{Q}(t)[x]$, and ϕ^d denotes the d-fold composition of ϕ with itself. The key property linking Φ_n to the above conjectures is that, for fixed $c \in \mathbb{Q}$, every algebraic number having period n under iteration of ϕ_c is a root of $\Phi_n(c, x)$, and conversely, every root of $\Phi_n(c, x)$ has period n under ϕ_c except in rare cases when the period may be smaller than n; see [Morton and Patel 1994, Theorem 2.4] for further details.

Questions about the points of period n under ϕ_c can thus be phrased as questions about the roots of $\Phi_n(c, x)$. It is therefore to be expected that a good understanding of the Galois group of $\Phi_n(c, x)$ will yield substantial information about the dynamical properties of the map ϕ_c. The results of the article [Krumm 2018b] provide an example of the type of information that can be obtained in this way. By a careful analysis of how the Galois group of $\Phi_4(c, x)$ can change as c varies in $\mathbb{Q}$, it is proved there that if $\alpha \in \overline{\mathbb{Q}}$ has period four under a map ϕ_c, then the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ can only be 2, 4, 8, or 12; in particular the degree cannot be 1, which implies that ϕ_c does not have a rational point of period 4. Furthermore, the Galois group data is used to show that $\delta(T_{4,c}) > 0.39$ for every $c \in \mathbb{Q}$, thus proving Conjecture 1.1 for $n = 4$. Motivated by these results, we are led to the following problem.

Problem 1.2. Let $G_{n,c}$ denote the Galois group of $\Phi_n(c, x)$ over $\mathbb{Q}$. For fixed n, determine the structure of all the groups $G_{n,c}$ as c varies in $\mathbb{Q}$.

Since the polynomials $\Phi_n(c, x)$ for $c \in \mathbb{Q}$ are specializations of Φ_n, it follows from Hilbert's irreducibility theorem [Serre 2008, Proposition 3.3.5] that for every rational number c outside a thin subset of $\mathbb{Q}$, the group $G_{n,c}$ is isomorphic to the Galois group of Φ_n over the function field $\mathbb{Q}(t)$. Moreover, by work of Bousch [1992, Chapter 3] it is known that Φ_n is irreducible and that its Galois group, which we denote by G_n, is isomorphic to a wreath product of a cyclic group and a symmetric group; indeed, $G_n \cong (\mathbb{Z}/n\mathbb{Z}) \wr S_r$, where $rn = \deg \Phi_n$. Hence, for most $c \in \mathbb{Q}$ the structure of $G_{n,c}$ is known. However, a complete solution of Problem 1.2 would require understanding precisely for which numbers c the specialization $t \mapsto c$ fails to preserve the Galois group of Φ_n. This raises a new but closely related problem.

Problem 1.3. For fixed n, determine all $c \in \mathbb{Q}$ such that $G_{n,c} \ncong G_n$.

Let $E_n = \{c \in \mathbb{Q} \mid G_{n,c} \ncong G_n\}$. By work of Morton [1992] and the author [Krumm 2018b], the sets E_n are well understood for $n \leq 4$; in particular, one notable feature of these sets is that they are infinite. In contrast, empirical evidence suggests that E_n is finite for every $n > 4$. The main purpose of this article is to prove this finiteness statement for several values of n.

Theorem 1.4. *The set E_n is finite if $n \in \{5, 6, 7, 9\}$.*

Using this theorem we can provide further evidence in support of Conjecture 1.1. It follows from the theorem that, for the above values of n, we have $G_{n,c} \cong (\mathbb{Z}/n\mathbb{Z}) \wr S_r$ for all but finitely many $c \in \mathbb{Q}$.

Excluding this finite set we therefore know the structure of all the Galois groups $G_{n,c}$. The Chebotarev density theorem can then be used to determine the value of $\delta(T_{n,c})$ by a straightforward calculation within the group $(\mathbb{Z}/n\mathbb{Z}) \wr S_r$. In this way we obtain the following result.

Theorem 1.5. *There exists a finite set $E \subset \mathbb{Q}$ such that the following lower bounds hold for every $c \in \mathbb{Q} \setminus E$:*

$$\delta(T_{5,c}) > 0.81, \quad \delta(T_{6,c}) > 0.84, \quad \delta(T_{7,c}) > 0.86, \quad \delta(T_{9,c}) > 0.89.$$

The proof of Theorem 1.4 relies on Hilbert's irreducibility theorem and Faltings's theorem to reduce the proof to a problem of showing that certain algebraic curves have genera greater than 1. More precisely, let S be a splitting field of Φ_n over $\mathbb{Q}(t)$, so that $G_n = \mathrm{Gal}(S/\mathbb{Q}(t))$, and let $\mathcal{X}$ be the smooth projective curve over $\mathbb{Q}$ whose function field is S. As explained in Section 2, in order to show that the set E_n is finite it suffices to show that, for every maximal proper subgroup $M < G_n$, the quotient curve $\mathcal{X}/M$ has genus greater than 1. Our main objective is therefore to compute the genera of these quotient curves, or at least to obtain lower bounds for them.

The methods we develop for this purpose allow us to reduce the problem to a series of computations within the groups G_n. For $n \in \{5, 6\}$ we are able to determine the genera exactly, and for $n \in \{7, 9\}$ we prove lower bounds which suffice for our purposes. Though the methods used here could in principle be used to extend our results to higher values of n, there are computational limitations which prevent this. For instance, the group G_{11} has order $11^{186}(186)!$ and the cost of computing its maximal subgroups is prohibitively expensive. Other computational issues are discussed in Section 7.

Though it would be desirable to explicitly determine the finite sets E_n in Theorem 1.4, our method of proof does not suggest a feasible way of doing this. Indeed, one would have to determine the sets of rational points on several curves of very large genera, a problem which seems impossible with current methods. Nevertheless, in Section 9 we make some elementary observations regarding the sets E_n; for instance, they are always nonempty.

This article is organized as follows. In Section 2 we establish two foundational results for the rest of the article. In Section 3 we prove a theorem concerning the structure of inertia groups in Galois extensions of valued fields; this may be of independent interest. In Section 4 we recall various properties of dynatomic polynomials which were mostly proved by P. Morton. In Section 5 we study the action of G_n on the roots of Φ_n. In Sections 6 and 7 we apply the results of earlier sections to carry out the genus computations from which Theorem 1.4 can be deduced. In Section 8 we prove Theorem 1.5. Finally, in Section 9 we list the known elements of the sets E_n.

2. Preliminaries

Let n be a positive integer and let Φ_n be the polynomial defined in (1-1). Let S be a splitting field of Φ_n over $\mathbb{Q}(t)$, and $G_n = \mathrm{Gal}(S/\mathbb{Q}(t))$. Recall that E_n denotes the set of all rational numbers c such that $G_{n,c} \ncong G_n$, where $G_{n,c}$ is the Galois group of $\Phi_n(c, x)$ over $\mathbb{Q}$. The following lemma provides sufficient conditions for E_n to be a finite set.

Lemma 2.1. *Let $M_1, \dots, M_s$ be representatives of all the conjugacy classes of maximal subgroups of G_n, and let L_i denote the fixed field of M_i. Suppose that every function field L_i has genus greater than* 1. *Then E_n is finite.*

Proof. Let $\mathcal{X}$ be the smooth projective curve with function field S, and for every index i, let $\mathcal{X}_i$ be the quotient curve $\mathcal{X}/M_i$. It follows from the proof of Proposition 3.3.1 in [Serre 2008] (see also [Krumm and Sutherland 2017, Theorem 1.1]) that there exist a finite set $\mathcal{E} \subset \mathbb{P}^1(\mathbb{Q})$ and morphisms $\pi_i : \mathcal{X}_i \to \mathbb{P}^1$ such that

$$E_n \subseteq \mathcal{E} \cup \bigcup_{i=1}^{s} \pi_i(\mathcal{X}_i(\mathbb{Q})).$$

Since L_i is the function field of $\mathcal{X}_i$, the hypotheses imply that the smooth projective model of $\mathcal{X}_i$ has genus greater than 1, and hence, by Faltings's theorem [1983], the set $\mathcal{X}_i(\mathbb{Q})$ is finite. The result follows immediately. □

In view of Lemma 2.1, the main objects of interest in this article are the genera of the minimal intermediate fields in the extension $S/\mathbb{Q}(t)$. Our first step towards understanding these genera will be to show that in computing them we may replace $\mathbb{Q}$ with any subfield of $\mathbb{C}$.

Proposition 2.2. *Let $\mathbb{F}$ be any field satisfying $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$, and let N be a splitting field of Φ_n over $\mathbb{F}(t)$. Then there is an isomorphism*

$$\iota : \mathrm{Gal}(N/\mathbb{F}(t)) \longrightarrow \mathrm{Gal}(S/\mathbb{Q}(t))$$

with the following property: if A is a subgroup of $\mathrm{Gal}(N/\mathbb{F}(t))$ and $B = \iota(A)$, then the fixed fields of A and B have the same genus.

Proof. Let Σ be a splitting field of Φ_n over $\mathbb{C}(t)$, and let $R \subset \Sigma$ be the set of roots of Φ_n. By basic field theory, we may identify N with the field $\mathbb{F}(t)(R)$ and S with the field $\mathbb{Q}(t)(R)$. Restriction of automorphisms then yields injective homomorphisms

$$\mathrm{Gal}(\Sigma/\mathbb{C}(t)) \hookrightarrow \mathrm{Gal}(N/\mathbb{F}(t)) \hookrightarrow \mathrm{Gal}(S/\mathbb{Q}(t)). \tag{2-1}$$

The group $\mathrm{Gal}(\Sigma/\mathbb{C}(t))$ is naturally isomorphic to a subgroup $G_{\mathbb{C}}$ of the symmetric group $\mathrm{Sym}(R)$. (Explicitly, the isomorphism is given by restriction to R.) Similarly, we define groups $G_{\mathbb{F}}$ and $G_{\mathbb{Q}}$. By (2-1) we have

$$G_{\mathbb{C}} \leq G_{\mathbb{F}} \leq G_{\mathbb{Q}} \leq \mathrm{Sym}(R). \tag{2-2}$$

The polynomial $\phi(x) = x^2 + t$ permutes the elements of R (see, for instance, [Krumm 2016, §2.2]); thus we may regard ϕ as an element of the group $\mathrm{Sym}(R)$. Let $\mathcal{C}$ denote the centralizer of ϕ in $\mathrm{Sym}(R)$. Since ϕ is a polynomial map, it commutes with every element of $\mathrm{Gal}(S/\mathbb{Q}(t))$, and therefore $G_{\mathbb{Q}} \leq \mathcal{C}$. Now, by Theorem 3 in [Bousch 1992, Chapter 3] we have $G_{\mathbb{C}} = \mathcal{C}$. Hence, (2-2) implies that $G_{\mathbb{C}} = G_{\mathbb{F}} = G_{\mathbb{Q}}$. It follows that the embeddings (2-1) are in fact isomorphisms; in particular, restriction to S is an isomorphism

$$\iota : \mathrm{Gal}(N/\mathbb{F}(t)) \xrightarrow{\sim} \mathrm{Gal}(S/\mathbb{Q}(t)). \tag{2-3}$$

We now digress briefly from the main proof.

Lemma 2.3. *The field $\mathbb{Q}$ is algebraically closed in S.*

Proof. Let k be the algebraic closure of $\mathbb{Q}$ in S. By general theory of algebraic function fields, the extension $k/\mathbb{Q}$ is finite; moreover, it can easily be shown to be a Galois extension. To see that $k/\mathbb{Q}$ is normal, let $p(x) \in \mathbb{Q}[x]$ be an irreducible polynomial having a root in k. Then p remains irreducible in $\mathbb{Q}(t)[x]$ (see Lemma 3.1.10 in [Stichtenoth 2009]) and has a root in S; therefore p splits in S. However, by definition of k, every root of p in S belongs to k. Hence, p splits in k.

Since $k(t)$ is the composite of k and $\mathbb{Q}(t)$, the extension $k(t)/\mathbb{Q}(t)$ is Galois, and restriction to k yields an isomorphism

$$\mathrm{Gal}(k(t)/\mathbb{Q}(t)) \cong \mathrm{Gal}(k/k \cap \mathbb{Q}(t)) = \mathrm{Gal}(k/\mathbb{Q}).$$

It follows that there is a surjective homomorphism $\mathrm{Gal}(S/\mathbb{Q}(t)) \to \mathrm{Gal}(k/\mathbb{Q})$ with kernel $H := \mathrm{Gal}(S/k(t))$. Now, taking $\mathbb{F} = k$ in (2-3), the image of ι is clearly contained in H, so that in fact $H = \mathrm{Gal}(S/\mathbb{Q}(t))$. Therefore $\mathrm{Gal}(k/\mathbb{Q})$ must be trivial, and $k = \mathbb{Q}$. □

Returning to the proof of the proposition, let $A \leq \mathrm{Gal}(N/\mathbb{F}(t))$ and set $B = \iota(A)$. Let U and V be the fixed fields of A and B, respectively. Thus, U and V are intermediate fields in the extensions $N/\mathbb{F}(t)$ and $S/\mathbb{Q}(t)$. We claim that U is the composite of V and $\mathbb{F}$. The fact that $U \supseteq V$ follows immediately from the definitions, and it is clear that $U \supseteq \mathbb{F}$; hence $U \supseteq V\mathbb{F}$. To prove that $U = V\mathbb{F}$ we will show that $[U : \mathbb{F}(t)] = [V\mathbb{F} : \mathbb{F}(t)]$. Since ι is an isomorphism mapping A to B, we have

$$[U : \mathbb{F}(t)] = |\mathrm{Gal}(N/\mathbb{F}(t)) : A| = |\mathrm{Gal}(S/\mathbb{Q}(t)) : B| = [V : \mathbb{Q}(t)].$$

Thus, it suffices to show that $[V : \mathbb{Q}(t)] = [V\mathbb{F} : \mathbb{F}(t)]$. Let α be a primitive element for V over $\mathbb{Q}(t)$, and let $p \in \mathbb{Q}(t)[x]$ be the minimal polynomial of α. Clearly $V\mathbb{F} = \mathbb{F}(t)(\alpha)$, so it is enough to show that p remains irreducible over $\mathbb{F}(t)$. Since p is irreducible over $\mathbb{Q}(t)$, the group $\mathrm{Gal}(S/\mathbb{Q}(t))$ acts transitively on the roots of p. This, together with the fact that ι is given by restriction to N, imply that $\mathrm{Gal}(N/\mathbb{F}(t))$ also acts transitively on the roots of p, and therefore p is irreducible over $\mathbb{F}(t)$. This completes the proof that $U = V\mathbb{F}$.

It remains only to show that U and V have the same genus. Since $\mathbb{F}$ contains the constant field of V (by Lemma 2.3), $U = V\mathbb{F}$ is a constant field extension of V (in the terminology of [Stichtenoth 2009, §3.6]). Equality between the genera of U and V now follows from Theorem 22 in [Artin 2006, p. 291]; see also Theorem 3.6.3 in [Stichtenoth 2009]. □

From Lemma 2.1 and Proposition 2.2 we deduce the following proposition, which is the key result of this section.

Proposition 2.4. *Let N be a splitting field of Φ_n over $\overline{\mathbb{Q}}(t)$. Let $M_1, \ldots, M_s$ be representatives of all the conjugacy classes of maximal subgroups of the group $G = \mathrm{Gal}(N/\overline{\mathbb{Q}}(t))$, and let L_i be the fixed field of M_i. Suppose that the genus of L_i is greater than 1 for every index i. Then the set E_n is finite.*

3. A result in valuation theory

Let K be a field, and let $v : K^* \to \mathbb{R}$ be a discrete valuation of K with perfect residue field k. Let N be a finite Galois extension of K with Galois group $G = \mathrm{Gal}(N/K)$. For any elements $\sigma, \tau \in G$ we will write τ^σ to denote the conjugate $\sigma^{-1}\tau\sigma$; similarly, for any subgroup $A \leq G$ we let $A^\sigma = \sigma^{-1}A\sigma$.

If L is an intermediate field in the extension N/K and w is a valuation of N extending a valuation u of L, we denote by $D_{w|u}$ and $I_{w|u}$ the decomposition and inertia groups of w over u. If u extends the valuation v of K, we let $e_{u|v}$ and $f_{u|v}$ denote the ramification index and residue degree of u over v.

Lemma 3.1. *Let w be a valuation of N extending v, and let $D = D_{w|v}$ and $I = I_{w|v}$. Let H be a subgroup of G with fixed field L, and let S_L be the set of all valuations of L extending v. Then there is a well-defined bijection*

$$D\backslash G/H \xrightarrow{\sim} S_L$$

given by $D\sigma H \mapsto (w \circ \sigma)|_L$. Furthermore, if $u = (w \circ \sigma)|_L$, then

$$e_{u|v} \cdot f_{u|v} = |D^\sigma : D^\sigma \cap H| \quad \textit{and} \quad e_{u|v} = |I^\sigma : I^\sigma \cap H|. \tag{3-1}$$

Proof. The first statement is well known; a proof may be found in Lemma 17.1.2 and Corollary 17.1.3 of [Efrat 2006]. Suppose now that $u = (w \circ \sigma)|_L$, and let $\tilde{w} = w \circ \sigma$. It is then a simple exercise to show that

$$D_{\tilde{w}|u} = D^\sigma \cap H \quad \text{and} \quad I_{\tilde{w}|u} = I^\sigma \cap H. \tag{3-2}$$

Note that $D^\sigma = D_{\tilde{w}|v}$ and $I^\sigma = I_{\tilde{w}|v}$. Now, since k is perfect, we have $|D_{\tilde{w}|v}| = e_{\tilde{w}|v} \cdot f_{\tilde{w}|v}$ and $|I_{\tilde{w}|v}| = e_{\tilde{w}|v}$ (see [Neukirch 1999, Chapter I, Proposition 9.6]). The relations (3-1) now follow easily from (3-2). □

Proposition 3.2. *Suppose that N is the splitting field of an irreducible polynomial $P(x) \in K[x]$. Let F be a subextension of N/K obtained by adjoining one root of $P(x)$ to K. Let $u_1, \ldots, u_m$ be the distinct valuations of F extending v, and set $e_i = e_{u_i|v}$ and $f_i = f_{u_i|v}$. Let w be a valuation of N extending v, and assume that $e_{w|v}$ is not divisible by the characteristic of k. Then the inertia group $I_{w|v}$ is generated by an element whose disjoint cycle decomposition (as a permutation of the roots of P) has the form*

$$\underbrace{(e_1\text{-cycle}) \cdots (e_1\text{-cycle})}_{f_1 \text{ times}} \cdots \underbrace{(e_m\text{-cycle}) \cdots (e_m\text{-cycle})}_{f_m \text{ times}}. \tag{3-3}$$

Proof. Set $D = D_{w|v}$ and $I = I_{w|v}$. The assumption that the characteristic of k does not divide $|I|$ implies that I is a cyclic group; see [Stichtenoth 2009, Proposition 3.8.5] or [Efrat 2006, §16.2]. Let R denote the set of roots of $P(x)$ in N, and consider the natural action of I on R. Let $\mathcal{O}$ be the set of orbits of this action. We will show that $\mathcal{O}$ can be partitioned into subsets $S_1, \ldots, S_m$ such that every orbit in S_i has cardinality e_i, and $\#S_i = f_i$. Note that this implies that every generator of I has a cycle decomposition of the form (3-3).

For every $x \in R$ let $\mathcal{O}_x$ and I_x, respectively, denote the orbit of x (under the action of I) and the stabilizer of x in I. Let $r \in R$ be such that $F = K(r)$, and set $H = \mathrm{Gal}(N/F)$. Note that H is the stabilizer of r in G.

By Lemma 3.1, there exist distinct double cosets $D\sigma_1 H, \dots, D\sigma_m H$ such that $u_i = (w \circ \sigma_i)|_F$. For $i = 1, \dots, m$ we define a map ψ_i as follows:

$$I^{\sigma_i} \backslash D^{\sigma_i} / (D^{\sigma_i} \cap H) \xrightarrow{\psi_i} \mathcal{O},$$
$$I^{\sigma_i} \tau (D^{\sigma_i} \cap H) \longmapsto \mathcal{O}_{\sigma_i \tau(r)}.$$

A straightforward calculation shows that ψ_i is well defined and injective. Letting $S_i \subseteq \mathcal{O}$ be the image of ψ_i, we claim that the sets $S_1, \dots, S_m$ have the properties stated above.

We begin by showing that every orbit in S_i has cardinality e_i. To ease notation, let us fix an index i and set $\sigma = \sigma_i$ and $M = D^\sigma \cap H$. Letting $\tau \in D^\sigma$, we must show that $\#\mathcal{O}_{\sigma\tau(r)} = e_i$. Note that $(I_{\sigma\tau(r)})^{\sigma\tau} = I^{\sigma\tau} \cap H$, so that $|I_{\sigma\tau(r)}| = |I^{\sigma\tau} \cap H|$, and therefore

$$\#\mathcal{O}_{\sigma\tau(r)} = |I : I_{\sigma\tau(r)}| = \frac{|I|}{|I_{\sigma\tau(r)}|} = \frac{|I^{\sigma\tau}|}{|I_{\sigma\tau(r)}|} = \frac{|I^{\sigma\tau}|}{|I_{\sigma\tau} \cap H|} = |I^{\sigma\tau} : I^{\sigma\tau} \cap H|.$$

Now, since $\tau \in D^\sigma$, we have $\sigma\tau \in D\sigma H$. Lemma 3.1 then implies that $(w \circ \sigma\tau)|_F = (w \circ \sigma)|_F = u_i$ and $|I^{\sigma\tau} : I^{\sigma\tau} \cap H| = e_i$. Hence $\#\mathcal{O}_{\sigma\tau(r)} = e_i$.

Next we show that $\#S_i = f_i$. Note that $\#S_i = \#I^\sigma \backslash D^\sigma / M$ since ψ_i is injective. The fact that I is a normal subgroup of D implies that

$$I^\sigma \backslash D^\sigma / M = D^\sigma / (I^\sigma M).$$

Thus, using Lemma 3.1 we obtain

$$\#S_i = |D^\sigma| / |I^\sigma M| = \frac{|D^\sigma| \cdot |I^\sigma \cap H|}{|D^\sigma \cap H| \cdot |I^\sigma|} = \frac{|D^\sigma : D^\sigma \cap H|}{|I^\sigma : I^\sigma \cap H|} = \frac{e_i f_i}{e_i} = f_i.$$

Now we show that the sets $S_1, \dots, S_m$ are pairwise disjoint. Suppose, by contradiction, that there exist distinct indices i, j such that $S_i \cap S_j \neq \varnothing$. Then there exist $\alpha \in D^{\sigma_i}$, $\beta \in D^{\sigma_j}$, and $\gamma \in I$ such that $\sigma_i \alpha(r) = \gamma \sigma_j \beta(r)$. Writing $\alpha = \sigma_i^{-1} \delta \sigma_i$ and $\beta = \sigma_j^{-1} d \sigma_j$ with $\delta, d \in D$, this implies that $\delta\sigma_i(r) = \gamma d \sigma_j(r)$; hence, there exists $h \in H$ such that $\sigma_i = \delta^{-1}\gamma d \sigma_j h$. Note that $\delta^{-1}\gamma d \in D$, so the previous equality implies that $\sigma_i \in D\sigma_j H$ and therefore $D\sigma_i H = D\sigma_j H$, a contradiction.

Finally, we show that $\mathcal{O} = \bigcup_{i=1}^m S_i$. Let $R_1, \dots, R_m$ be the subsets of R defined by $R_i = \bigcup_{C \in S_i} C$. From the results proved above it follows that $\#R_i = e_i f_i$ and that the sets $R_1, \dots, R_m$ are pairwise disjoint. Given that v is a discrete valuation, we have the relation $[F : K] = \sum_{i=1}^m e_i f_i$. Hence

$$\#R = \deg(P) = [F : K] = \sum_{i=1}^m e_i f_i = \sum_{i=1}^m \#R_i = \#\bigcup_{i=1}^m R_i.$$

It follows that $R = \bigcup_{i=1}^m R_i$, which implies that $\mathcal{O} = \bigcup_{i=1}^m S_i$. □

Remark 3.3. Proposition 3.2 was inspired by a theorem of Beckmann [1994] concerning inertia groups in Galois extensions of $\mathbb{Q}$; indeed, Beckmann's result is essentially the case $K = \mathbb{Q}$ of the proposition. However, the proof given here has little in common with the proof in [loc. cit.].

Proposition 3.4. *With notation and assumptions as in Proposition 3.2, let γ be a generator of $I_{w|v}$ and let H be a subgroup of G with fixed field L. Suppose that $D_{w|v} = I_{w|v}$. Then the number of valuations u of L extending v such that $e_{u|v} = 1$ is given by*

$$\frac{|C_G(\gamma)| \cdot s(H, \gamma)}{|H|}, \tag{3-4}$$

where $C_G(\gamma)$ is the centralizer of γ in G and $s(H, \gamma)$ is the number of G-conjugates of γ that belong to H.

Proof. Let $D = D_{w|v}$ and define sets $A = \{\sigma \in G \mid \gamma^\sigma \in H\}$ and

$$\Delta = \{D\sigma H \in D\backslash G/H \mid \sigma \in A\}.$$

It follows from Lemma 3.1 that the cardinality of Δ is equal to the number of valuations u of L extending v such that $e_{u|v} = 1$. Thus, in order to prove the proposition it suffices to show that $|H| \cdot (\#\Delta) = |C_G(\gamma)| \cdot s(H, \gamma)$.

For every element $a \in A$ the right coset $C_G(\gamma)\cdot a$ is contained in A; hence, the set $U = \{C_G(\gamma)\cdot a \mid a \in A\}$ is a partition of A into subsets of size $|C_G(\gamma)|$. Thus $\#A = |C_G(\gamma)| \cdot (\#U)$. Now let $B = \{\gamma^\sigma \mid \sigma \in G\} \cap H$, so that $\#B = s(H, \gamma)$. Note that $\#U = \#B$; indeed, there is a bijective map $U \to B$ given by $C_G(\gamma)\cdot a \mapsto \gamma^a$. Therefore,

$$\#A = |C_G(\gamma)| \cdot (\#B) = |C_G(\gamma)| \cdot s(H, \gamma). \tag{3-5}$$

Let $f : A \twoheadrightarrow \Delta$ be the surjective map given by $f(\sigma) = D\sigma H$. We claim that, for every $a \in A$, $f^{-1}(f(a)) = aH$. It is clear that $aH \subseteq f^{-1}(f(a))$. Now suppose that $f(a') = f(a)$, so that $a' = dah$ for some $d \in D$ and $h \in H$. Since $\gamma^a \in H$, we may write $\gamma a = ah'$ for some $h' \in H$. Furthermore, since $D = I_{w|v} = \langle\gamma\rangle$, we have $d = \gamma^n$ for some positive integer n. Thus

$$a' = dah = \gamma^n ah = a(h')^n h \in aH,$$

which proves the claim. Since every fiber of f has cardinality $|H|$, we have $\#A = |H| \cdot (\#\Delta)$, and hence, by (3-5), $|H| \cdot (\#\Delta) = |C_G(\gamma)| \cdot s(H, \gamma)$. □

For later reference, we include here a combined statement of Propositions 3.2 and 3.4 in the special case where K is the function field $\overline{\mathbb{Q}}(t)$ and the valuation v corresponds to a place p of K. Note that in this case all residue degrees $f_{u|v}$ are equal to 1.

Corollary 3.5. *Let t be an indeterminate and $K = \overline{\mathbb{Q}}(t)$. Suppose that $P(x) \in K[x]$ is irreducible, and let N be a splitting field for $P(x)$. Let F be a subextension of N/K obtained by adjoining one root of $P(x)$ to K. Let p be a place of K, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the distinct places of F lying over p. Then, for every place $\mathfrak{P}$ of N lying over p, the inertia group $I_{\mathfrak{P}|p}$ is generated by an element γ whose disjoint cycle decomposition has the form $(e_1\text{-cycle}) \cdots (e_m\text{-cycle})$, where e_i is the ramification index of $\mathfrak{p}_i$ over p. Furthermore, if H is a subgroup of $G = \mathrm{Gal}(N/K)$ with fixed field L, then the number of places of L lying over p which are unramified over K is given by the formula (3-4).*

4. Ramification data for dynatomic polynomials

Let us fix a positive integer n. We will henceforth regard the polynomial $\Phi_n(x)$ as an element of the ring $\overline{\mathbb{Q}}(t)[x]$. As such, it is known by work of Bousch [1992, Chapter 3] that Φ_n is irreducible. In this section we will apply Corollary 3.5 to study inertia groups in the Galois group of Φ_n.

Let $K = \overline{\mathbb{Q}}(t)$, let N/K be a splitting field of Φ_n, and let $G = \mathrm{Gal}(N/K)$. Let F be a subextension of N/K obtained by adjoining one root of Φ_n to K. Morton [1996, §3] studies the ramification of places in the extension F/K by using certain polynomials $\Delta_{n,d} \in \mathbb{Z}[t]$, where d is a divisor of n. These polynomials had previously been defined in [Morton and Vivaldi 1995, §1]; we refer the reader to that article for the definition. We now recall a few results from [Morton 1996; Morton and Vivaldi 1995] which will be needed here.

For every positive integer s, let

$$\nu(s) = \tfrac{1}{2} \sum_{d \mid s} \mu(s/d) 2^d.$$

Lemma 4.1 (Morton–Vivaldi). *For every divisor d of n, let $R_{n,d} \subset \overline{\mathbb{Q}}$ denote the set of roots of $\Delta_{n,d}$. Then the following hold*:

(a) $\#R_{n,d} = \deg \Delta_{n,d}$ *for every* d.

(b) *If d and e are distinct divisors of n, then $R_{n,d} \cap R_{n,e} = \varnothing$.*

(c) *Letting φ denote Euler's phi function, the degree of $\Delta_{n,d}$ is given by*

$$\deg \Delta_{n,d} = \begin{cases} \nu(d)\varphi(n/d) & \text{if } d < n, \\ \nu(n) - \sum_{\substack{k \mid n \\ k<n}} \nu(k)\varphi(n/k) & \text{if } d = n. \end{cases}$$

Proof. All statements are proved in [Morton and Vivaldi 1995]. Indeed, (a) and (b) follow from Proposition 3.2, and (c) follows from Corollary 3.3. □

Recall that for every place p of K, the *conorm* of p with respect to the extension F/K is the divisor, which we write multiplicatively, defined by

$$i_{F/K}(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are the distinct places of F lying over p and e_i is the ramification index of $\mathfrak{p}_i$ over p. A discussion of the basic properties of the conorm map may be found in [Stichtenoth 2009, §3.1] or [Rosen 2002, Chapter 7].

Let $D = \deg \Phi_n$; note that $D = 2\nu(n)$. As explained in Section 5, the set of roots of Φ_n can be partitioned into sets of cardinality n, and therefore n divides D. Let $r = D/n$.

Lemma 4.2 (Morton). *Let p_∞ be the infinite place of K, i.e., the place corresponding to the valuation v_∞ of K given by $v_\infty(f/g) = \deg g - \deg f$. For $b \in \overline{\mathbb{Q}}$, let p_b denote the place of K corresponding to the polynomial $t - b$.*

(a) *The places of K that ramify in F are p_∞ and p_b for $b \in \bigcup_{d \mid n} R_{n,d}$.*

(b) *The conorm of p_∞ has the form*

$$i_{F/K}(p_\infty) = \mathfrak{p}_1^2 \cdots \mathfrak{p}_{\nu(n)}^2.$$

(c) *For every $b \in R_{n,n}$, the conorm of p_b has the form*

$$i_{F/K}(p_b) = \mathfrak{p}_1^2 \cdots \mathfrak{p}_n^2 \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_{n(r-2)}.$$

(d) *For every $b \in R_{n,d}$, where $d < n$, the conorm of p_b has the form*

$$i_{F/K}(p_b) = \mathfrak{p}_1^{n/d} \cdots \mathfrak{p}_d^{n/d} \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_{n(r-1)}.$$

Proof. All statements are proved in [Morton 1996]; (a), (c) and (d) follow from the proof of Proposition 9, and (b) follows from Proposition 10. □

Let $\mathbb{P} = \{p_\infty\} \cup \left\{p_b \mid b \in \bigcup_{d \mid n} R_{n,d}\right\}$ be the set of places of K that ramify in F. For any intermediate field L in the extension N/K and any place p of K, let $\mathbb{P}_L(p)$ denote the set of places of L lying over p.

We introduce some terminology to be used throughout the article. Suppose that G is a group acting on a finite set X, and let $g \in G$. We say that g has *cycle type* (a, b), where a and b are positive integers, if the disjoint cycle decomposition of g, disregarding 1-cycles, is a product of b a-cycles.

Applying Corollary 3.5 to the polynomial Φ_n and using Lemma 4.2, we immediately obtain the following description of inertia groups in G.

Proposition 4.3. *Let $p \in \mathbb{P}$ and $\mathfrak{P} \in \mathbb{P}_N(p)$. Then the inertia group $I_{\mathfrak{P} \mid p}$ has a generator with cycle type (a, b) satisfying*

$$(a, b) = \begin{cases} (2, D/2) & \text{if } p = p_\infty, \\ (2, n) & \text{if } p = p_b \text{ with } b \in R_{n,n}, \\ (n/d, d) & \text{if } p = p_b \text{ with } b \in R_{n,d},\ d < n. \end{cases}$$

In addition to the data on ramification of places in F/K provided by Lemma 4.2, in later sections we will need some ramification data for a subfield $F_0 \subset F$ defined as follows. Let θ be a root of Φ_n such that $F = K(\theta)$. The field F has an automorphism[1] given by $\theta \mapsto \phi(\theta) = \theta^2 + t$; we define F_0 to be the fixed field of this automorphism.

Proposition 4.4 (Morton). *Let $p \in \mathbb{P}$ and let $S(p) = \sum_{\mathfrak{q} \in \mathbb{P}_{F_0}(p)} (e_{\mathfrak{q} \mid p} - 1)$.*

(a) *If $p = p_\infty$, then $S(p) = r - e_n$, where*

$$e_n = \frac{1}{2n} \sum_{d \mid (n,2)} \varphi(d)^2 \cdot \sum_{k \in U_{n,d}} \mu(n/k) 2^{k/d}.$$

Here $U_{n,d} = \{k \in \mathbb{Z}_{>0} : k \mid n, d \mid k, \text{ and } (n/k, d) = 1\}$.

(b) *If $p = p_b$, where $b \in R_{n,n}$, then $S(p) = 1$.*

(c) *If $p = p_b$, where $b \in R_{n,d}$ for some $d < n$, then $S(p) = 0$.*

[1] Note that $\phi(\theta)$ is a root of Φ_n, so there is an isomorphism $F \to K(\phi(\theta))$ mapping θ to $\phi(\theta)$. Moreover, the fact that $\phi^n(\theta) = \theta$ implies that $F = K(\phi(\theta))$, so this map is in fact an automorphism of F.

Proof. All statements are proved in [Morton 1996]; (a) follows Theorem 13, while (b) and (c) can be deduced from the proof of Proposition 9. Indeed, it is shown in that proposition that if $p = p_b$, where $b \in R_{n,n}$, then there is a unique ramified place of F_0 lying over p, and its ramification index is 2; this implies (b). Similarly, if $p = p_b$, where $b \in R_{n,d}$ for some $d < n$, then p is unramified in F_0, which implies (c). □

5. The action of the Galois group of Φ_n

We continue using here the notation introduced in the previous section. The genus computations in Sections 6 and 7, which form the core of this article, rely fundamentally on Propositions 3.4 and 4.3. In order to apply these propositions effectively, we require a precise understanding of the elements of G whose cycle decompositions have the forms described in Proposition 4.3. In addition, explicit formulas for the orders of the centralizers of these elements will be needed when applying Proposition 3.4. The purpose of this section is to carry out a detailed analysis of the action of G on the roots of Φ_n. In the process we address both of the above requirements, the key result being Proposition 5.5.

Recall the notion of an isomorphism of group actions: if A and B are groups acting on sets X and Y, respectively, we write $A \equiv B$ if there exist a group isomorphism $\varphi : A \to B$ and a bijection $\varepsilon : X \to Y$ such that $\varepsilon(ax) = \varphi(a)\varepsilon(x)$ for all $a \in A$ and $x \in X$. Though the notation $A \equiv B$ does not make reference to the sets X and Y, this should cause no confusion here because the sets being acted on will be clear from context.

Let R be the set of roots of Φ_n in the splitting field N, and consider the natural action of G on R. In this section we will discuss three group actions, which we refer to as *realizations* of G, that are isomorphic to G with its action on R. The first realization is the automorphism group of a graph acting on its set of vertices; this is helpful as a visual aid for understanding the action of G. The second realization is a particular subgroup of the symmetric group S_D acting on the set $\{1, \dots, D\}$; this is useful for carrying out explicit computations with elements of G. The third realization is a wreath product $(\mathbb{Z}/n\mathbb{Z}) \wr S_r$ acting on the set $(\mathbb{Z}/n\mathbb{Z}) \times \{1, \dots, r\}$. Though somewhat more technical, we find that this realization is the most convenient for purposes of proving the main results of this section. The key fact needed to show that these realizations are isomorphic is a well-known theorem of Bousch [1992, Chapter 3], namely Theorem 3.

5A. ***The group G as a graph automorphism group.*** It is a simple consequence of the definition of Φ_n that the map $\phi(x) = x^2 + t$ permutes the elements of R (see [Krumm 2016, §2.2] for details). Regarding ϕ as an element of the symmetric group $\mathrm{Sym}(R)$, we may therefore partition the set R into ϕ-orbits. By [Morton and Patel 1994, Theorem 2.4(c)], the fact that Φ_n is irreducible implies that every orbit has size n; hence, the number of orbits is $(\#R)/n = D/n = r$.

Let $\mathcal{G}$ be the natural embedding of G in $\mathrm{Sym}(R)$, and note that $G \equiv \mathcal{G}$. Let Γ be the directed graph whose vertices are the elements of R and which has an edge $x \to \phi(x)$ for every $x \in R$. An illustration of Γ is shown in Figure 1 below. By Bousch's theorem, $\mathcal{G}$ is the centralizer of ϕ in $\mathrm{Sym}(R)$. (More explicitly, this is a consequence of the proof of Proposition 2.2. In the notation of that proof, we have $\mathcal{G} = G_{\mathbb{F}}$, where $\mathbb{F} = \overline{\mathbb{Q}}$.) It follows that $\mathcal{G} = \mathrm{Aut}(\Gamma)$ and therefore $G \equiv \mathrm{Aut}(\Gamma)$.

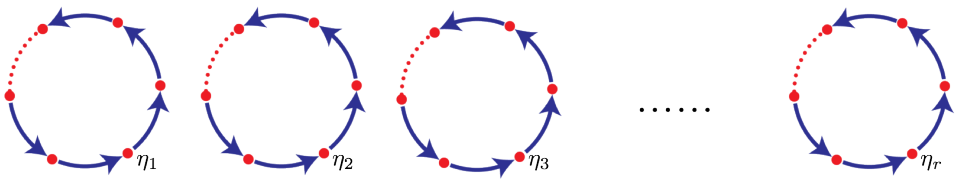

Figure 1. A directed graph whose automorphism group is isomorphic to the Galois group of Φ_n. Every cycle in the graph has n vertices, and there are r cycles in total.

5B. ***The group G as a permutation group.*** Let S_D be the symmetric group on the set $\{1, \dots, D\}$ and let $\sigma \in S_D$ be the permutation defined by

$$\sigma = (1, \dots, n)(n+1, \dots, 2n) \cdots (D-n+1, \dots, D).$$

There is a bijection $\ell : \{1, \dots, D\} \to R$ under which the cycles in the decomposition of σ correspond to the cycles in the graph Γ. Indeed, if we choose representatives $\eta_1, \dots, \eta_r$ of the distinct cycles in Γ, then one such map ℓ is given by

$$\ell(ni - j) = \phi^{n-j}(\eta_i) \quad \text{for } 1 \le i \le r \text{ and } 0 \le j < n.$$

The map ℓ induces an isomorphism $\iota : S_D \to \mathrm{Sym}(R)$ under which σ maps to ϕ. Let $\mathcal{Z}$ be the centralizer of σ in S_D. Since $\mathcal{G}$ is the centralizer of ϕ in $\mathrm{Sym}(R)$, the image of $\mathcal{Z}$ under ι is equal to $\mathcal{G}$. Moreover, the maps ι and ℓ induce an isomorphism of group actions between $\mathcal{Z}$ and $\mathcal{G}$; hence $G \equiv \mathcal{Z}$.

5C. ***Background on wreath products.*** Before discussing the realization of G as a wreath product, we recall the basic construction of wreath products. For further information on this topic we refer the reader to [Dixon and Mortimer 1996, §2.6; Rotman 1995, Chapter 7; Kerber 1971, Chapter I].

Let S_r denote the symmetric group on the set $\Omega = \{1, \dots, r\}$. Let A be a group, and consider the direct product A^r consisting of functions $f : \Omega \to A$ with pointwise multiplication. There is an action of S_r on A^r given by $\pi \cdot f = f_\pi$, where f_π is the function

$$f_\pi(i) = f(\pi^{-1}(i)) \quad \text{for every } i \in \Omega.$$

This action induces a homomorphism $S_r \to \mathrm{Aut}(A^r)$, so we may form the semidirect product $\mathcal{W} = A^r \rtimes S_r$. Elements of $\mathcal{W}$ have the form (f, π), where $f \in A^r$ and $\pi \in S_r$; the group operation in $\mathcal{W}$ is given by

$$(f, \pi)(g, \sigma) = (f g_\pi, \pi\sigma).$$

The group $\mathcal{W}$ is the wreath product of A with S_r, denoted $A \wr S_r$. Letting e and 1, respectively, denote the identity elements of A^r and S_r, there are embeddings $A^r \hookrightarrow \mathcal{W}$ and $S_r \hookrightarrow \mathcal{W}$ given by $f \mapsto (f, 1)$ and $\pi \mapsto (e, \pi)$; we will henceforth identify A^r and S_r with their images under these maps. The group $B = A^r$, called the *base group* of the wreath product, is a normal subgroup of $\mathcal{W}$; indeed, B is the kernel

of the projection map $\mathcal{W} \to S_r$ given by $(f, \pi) \mapsto \pi$. Furthermore, S_r is a complement for B in the sense that $B \cap S_r$ is trivial and $BS_r = \mathcal{W}$.

Suppose now that A acts on a set Δ. Then there is an action of $\mathcal{W}$ on the Cartesian product $\Delta \times \Omega$ given by

$$(f, \pi) \cdot (d, i) = (f(\pi(i)) \cdot d, \pi(i)). \tag{5-1}$$

Moreover, this action is faithful if A acts faithfully on Δ.

5D. ***The group G as a wreath product.*** For the remainder of this section we assume that $A = \mathbb{Z}/n\mathbb{Z}$, so that $\mathcal{W} = (\mathbb{Z}/n\mathbb{Z}) \wr S_r$. The action of A on itself by addition induces a faithful action of $\mathcal{W}$ on the set $X = A \times \Omega$ given by (5-1). We will show that $\mathcal{W} \equiv G$.

Let $\eta_1, \ldots, \eta_r$ be representatives of the distinct ϕ-orbits of R. For every $w = (f, \pi) \in \mathcal{W}$ we define $\zeta_w \in \mathcal{G} = \mathrm{Aut}(\Gamma)$ by

$$\zeta_w(\phi^a(\eta_i)) = \phi^{f(\pi(i))+a}(\eta_{\pi(i)}) \quad \text{for } a \in A \text{ and } i \in \Omega.$$

Note that the notation ϕ^a for $a \in A$ is unambiguous since ϕ^n is the identity element of $\mathrm{Sym}(R)$. Using the fact that $\mathcal{G}$ is the centralizer of ϕ in $\mathrm{Sym}(R)$, it is a simple exercise to show that ζ_w is a well-defined element of $\mathcal{G}$, and that the map $\zeta : \mathcal{W} \to \mathcal{G}$ given by $w \mapsto \zeta_w$ is a group isomorphism.

Let $\varepsilon : X \to R$ be the map defined by $\varepsilon(a, i) = \phi^a(\eta_i)$. From the definitions it follows that ε is a bijection and that for every $w \in \mathcal{W}$ and $\alpha \in X$ we have $\varepsilon(w\alpha) = \zeta(w)\varepsilon(\alpha)$. Hence $\mathcal{W} \equiv \mathcal{G}$, and therefore $G \equiv \mathcal{W}$. Using this realization of G as a wreath product, we will now study the action of G.

Remark 5.1. It follows from the above discussion that

$$\mathrm{Aut}(\Gamma) \cong (\mathbb{Z}/n\mathbb{Z}) \wr S_r.$$

This is a special case of a well-known theorem of Frucht in graph theory. As shown in [Frucht 1949] (see also [Harary 1969, Theorem 14.5]), if Λ is a finite connected graph and Γ is a graph consisting of r disjoint copies of Λ, then $\mathrm{Aut}(\Gamma) \cong \mathrm{Aut}(\Lambda) \wr S_r$.

5E. ***Conjugacy in $\mathcal{W}$.*** Our main reason for using the realization of G as a wreath product is that it provides convenient ways of deciding whether two elements of G are conjugates of each other, and of calculating the order of the centralizer of any element of G. The key notion needed for these tasks is the *type* of an element of $\mathcal{W}$, defined below.

For every cycle $C = (i_1, i_2, \ldots, i_k) \in S_r$ and every element $f \in A^r$, we denote by $f(C)$ the element of A given by $f(C) = f(i_1) + \cdots + f(i_k)$.

For every element $w = (f, \pi) \in \mathcal{W}$, we define a map $T_w : X \to \mathbb{Z}_{\geq 0}$ as follows: for $a \in A$ and $k \in \Omega$, $T_w(a, k)$ is the number of k-cycles C in the cycle decomposition of π such that $f(C) = a$. The map T_w will be called the *type* of w. When w is clear from context, we will denote $T_w(a, k)$ simply by t_{ak} and we will use matrix notation (t_{ak}) to denote the map T_w.

Proposition 5.2. (1) *Let $w_1, w_2 \in \mathcal{W}$. Then w_1 and w_2 are conjugates if and only if they have the same type.*

(2) *If w has type (t_{ak}), then the order of the centralizer of w in $\mathcal{W}$ is given by the formula*

$$\prod_{a\in A}\prod_{k\in\Omega}(t_{ak})!(kn)^{t_{ak}}.$$

Proof. Both statements can be deduced from more general results proved in [Kerber 1971]. Specifically, (1) follows from item 3.7 on page 44, and (2) follows from item 3.9 on page 47. □

5F. ***The action of $\mathcal{W}$.*** In this section we prove various properties of the action of $\mathcal{W}$ on X. For elements $w = (f, \pi) \in \mathcal{W}$ and $\alpha = (a, i) \in X$, we will denote by $w(\alpha)$ the action of w on α. Thus,

$$w(\alpha) = (f(\pi(i)) + a, \pi(i)). \tag{5-2}$$

Let $C_i = A \times \{i\}$ for $1 \le i \le r$. Under the map ε defined in Section 5D, C_i corresponds to the i-th cycle in the graph Γ, i.e., the cycle containing η_i.

The base group $A^r \le \mathcal{W}$ is generated by the elements $\rho_1, \dots, \rho_r$ defined by $\rho_i = (\delta_i, 1)$, where $\delta_i(j) = 0$ if $j \ne i$ and $\delta_i(i) = 1$. Note that ρ_i maps C_i to itself and acts as the identity on C_j if $j \ne i$. Viewed as an element of $\mathrm{Aut}(\Gamma)$ (via the map ζ defined in Section 5D), ρ_i acts as a $1/n$ rotation on the i-th cycle. Let $\rho = \rho_1 \cdots \rho_r = (\delta, 1)$, where $\delta(i) = 1$ for all $i \in \Omega$. Then $\zeta(\rho) = \phi$, so ρ is in the center of $\mathcal{W}$. A simple calculation shows that for all $s \in \mathbb{Z}$, $a \in A$, and $i \in \Omega$ we have

$$\rho^s(a, i) = \rho_i^s(a, i) = (a + \bar{s}, i). \tag{5-3}$$

For every $w \in \mathcal{W}$ and every $i \in \Omega$, let $w(C_i) = \{w(\alpha) \mid \alpha \in C_i\}$.

Lemma 5.3. *Let $w = (f, \pi) \in \mathcal{W}$ and let $i \in \Omega$.*

(1) *Letting $j = \pi(i)$, we have $w(C_i) = C_j$.*

(2) *If $w(C_i) = C_i$, then there exists $0 \le s < n$ such that $w(\alpha) = \rho_i^s(\alpha)$ for every $\alpha \in C_i$. Moreover, the w-orbit of every element of C_i has cardinality $n/\gcd(n, s)$.*

Proof. For every element $(a, i) \in C_i$ we have $w(a, i) = (f(j) + a, j) \in C_j$, so $w(C_i) \subseteq C_j$. Since $\#C_i = \#C_j$ and w acts as a bijection on X, this implies that $w(C_i) = C_j$, proving (1). Suppose now that $w(C_i) = C_i$, and let $0 \le s < n$ be such that $w(0, i) = (\bar{s}, i)$. By (5-3) we have $w(0, i) = \rho^s(0, i)$. Given $\alpha \in C_i$, we may write α in the form $\alpha = (\bar{k}, i) = \rho^k(0, i)$ for some integer k. Using (5-3) and the fact that w commutes with ρ we obtain

$$w(\alpha) = w\rho^k(0, i) = \rho^k w(0, i) = \rho^k\rho^s(0, i) = \rho^s\rho^k(0, i) = \rho^s(\alpha) = \rho_i^s(\alpha).$$

This proves the first statement in (2). Since w acts like ρ_i^s on C_i, the orbit of α under w is equal to its orbit under ρ_i^s. The cyclic group generated by ρ_i^s has order $n/\gcd(n, s)$, and it follows from (5-3) that the stabilizer of α in this group is trivial; hence the orbit of α has cardinality $n/\gcd(n, s)$. This completes the proof of (2). □

Lemma 5.4. *Let $w = (f, \pi) \in \mathcal{W}$. Suppose that $i, j \in \Omega$ are such that $w(C_i) = C_j$, $w(C_j) = C_i$, and $w^2(\alpha) = \alpha$ for every $\alpha \in C_i \cup C_j$. Then there exists $0 \le s < n$ such that $w(\alpha) = \rho_i^{-s}\pi\rho_i^s(\alpha)$ for every $\alpha \in C_i \cup C_j$.*

Proof. Let $w(0, i) = (\bar{s}, j)$ and $w(0, j) = (\bar{t}, i)$ with $0 \le s, t < n$. From (5-3) and the fact that w commutes with ρ it follows that for every integer k we have $w(\bar{k}, i) = (\bar{s} + \bar{k}, j)$ and $w(\bar{k}, j) = (\bar{t} + \bar{k}, i)$. Using this we calculate $w^2(0, i) = w(\bar{s}, j) = (\bar{t} + \bar{s}, i)$. Since $w^2(0, i) = (0, i)$, this implies that $\bar{t} = -\bar{s}$; thus, for every integer k we have

$$w(\bar{k}, i) = (\bar{k} + \bar{s}, j) \quad \text{and} \quad w(\bar{k}, j) = (\bar{k} - \bar{s}, i). \tag{5-4}$$

Since $w(C_i) = C_j$ and $w(C_j) = C_i$, Lemma 5.3 implies that $\pi(i) = j$ and $\pi(j) = i$. It follows that for every $a \in A$ we have $\pi(a, i) = (a, j)$ and $\pi(a, j) = (a, i)$. Let $w' = \rho_i^{-s}\pi\rho_i^s$. If $\alpha = (\bar{k}, i) \in C_i$, then a simple calculation shows that $w'(\alpha) = (\bar{k} + \bar{s}, j)$, so $w'(\alpha) = w(\alpha)$ by (5-4). Similarly, if $\alpha = (\bar{k}, j) \in C_j$, then $w'(\alpha) = (\bar{k} - \bar{s}, i) = w(\alpha)$. Therefore $w(\alpha) = \rho_i^{-s}\pi\rho_i^s(\alpha)$ for every $\alpha \in C_i \cup C_j$. □

We can now prove the main result of this section.

Proposition 5.5. *Let $w \in \mathcal{W}$ and let $\mathcal{C}$ be the centralizer of w in $\mathcal{W}$.*

(1) *Suppose that w has cycle type $(2, D/2)$. Then the following hold*:
   (a) *Assume that $w(C_i) \ne C_i$ for all $i \in \Omega$. Then r is even, w is conjugate to the permutation $(1, 2)(3, 4)\cdots(r-1, r) \in S_r$, and $|\mathcal{C}| = (r/2)!(2n)^{r/2}$.*
   (b) *Assume $w(C_i) = C_i$ for some $i \in \Omega$. Then n is even and there exists $0 < \ell \le r$ such that $r - \ell$ is even and w is conjugate to the element $(\rho_1 \cdots \rho_\ell)^{n/2}\varepsilon$, where $\varepsilon = (\ell+1, \ell+2)\cdots(r-1, r) \in S_r$. Moreover, we have $|\mathcal{C}| = \ell!((r-\ell)/2)!n^\ell(2n)^{(r-\ell)/2}$.*

(2) *Suppose that w has cycle type $(2, n)$. Then the following hold*:
   (a) *Assume $w(C_i) = C_i$ for all $i \in \Omega$. Then n is even, there exist indices $i < j \in \Omega$ such that $w = (\rho_i\rho_j)^{n/2}$, and $|\mathcal{C}| = 2(r-2)!n^r$.*
   (b) *Assume $w(C_i) \ne C_i$ for some $i \in \Omega$. Then there exist indices $i < j \in \Omega$ and an integer $0 \le s < n$ such that $w = \rho_i^{-s}\tau\rho_i^s$, where $\tau = (i, j) \in S_r$. In this case, $|\mathcal{C}| = 2(r-2)!n^{r-1}$.*

(3) *Suppose that w moves exactly n elements of X. Then $w = \rho_i^s$ for some $i \in \Omega$ and some integer $0 < s < n$. Moreover, $|\mathcal{C}| = (r-1)!n^r$.*

Proof. Let $f \in A^r$ and $\pi \in S_r$ be such that $w = (f, \pi)$, and let (t_{ak}) be the type of w. We begin by proving 1(a). The hypothesis in (1) together with the fact that $\mathcal{W}$ acts faithfully on X imply that $w^2 = (f + f_\pi, \pi^2)$ is the identity element $(e, 1)$; in particular, $\pi^2 = 1$. Moreover, by Lemma 5.3 we have $w(C_i) = C_{\pi(i)}$ for every $i \in \Omega$, so $\pi(i) \ne i$ for every i. Hence the π-orbit of every element of Ω has cardinality 2. It follows that r is even, say $r = 2m$, and π is a product of m disjoint transpositions. We can now determine the type of w.

Let $\{i_1, \pi(i_1)\}, \ldots, \{i_m, \pi(i_m)\}$ be the orbits of π. Since π has no k-cycles if $k = 1$ or $k > 2$, then $t_{ak} = 0$ for all such k. When $k = 2$, t_{ak} is the number of indices $1 \le v \le m$ such that $f(i_v) + f(\pi(i_v)) = a$. Since

$\pi^2 = 1$, this is equivalent to $f(i_v) + f_\pi(i_v) = a$. Now, as mentioned above, $w^2 = (f + f_\pi, \pi^2) = (e, 1)$, so $f + f_\pi = e$ and therefore $f(i) + f_\pi(i) = 0$ for every $i \in \Omega$. Hence, the condition $f(i_v) + f_\pi(i_v) = a$ is equivalent to $a = 0$. Thus we have $t_{a2} = 0$ if $a \neq 0$, and $t_{02} = m$. This determines the type of w. It is now trivial to check that w has the same type as the permutation $\tau = (1, 2)(3, 4) \cdots (r - 1, r) \in S_r$. It follows from Proposition 5.2 that w is conjugate to τ and that $|\mathcal{C}| = m!(2n)^m$; this completes the proof of 1(a).

Next we prove 1(b). Suppose that $i \in \Omega$ satisfies $w(C_i) = C_i$. By Lemma 5.3, there exists $0 \leq s < n$ such that w acts like ρ_i^s on C_i, and the w-orbit of every element of C_i has cardinality $n/\gcd(n, s)$. By hypothesis every orbit has size 2, so $n/\gcd(n, s) = 2$, and hence n must be even and $s = n/2$.

Let $i_1, \ldots, i_\ell$ be all the indices i in Ω such that $w(C_i) = C_i$. Clearly, $0 < \ell \leq r$. Arguing as in the proof of 1(a), we see that π fixes i_k for each k, and that if $i \in \Omega \setminus \{i_1, \ldots, i_\ell\}$, then the orbit of i under π has size 2. This implies that $r - \ell$ is even, say $r - \ell = 2q$, and the disjoint cycle decomposition of π is a product of ℓ 1-cycles and q transpositions. The type of w is now easy to determine as done in case 1(a).

Clearly, $t_{ak} = 0$ if $k > 2$. Let $\{i_1\}, \ldots, \{i_\ell\}, \{j_1, \pi(j_1)\}, \ldots, \{j_q, \pi(j_q)\}$ be the orbits of π. Then t_{a2} is the number of indices $1 \leq v \leq q$ such that $f(j_v) + f_\pi(j_v) = a$. But $f + f_\pi = e$, so $t_{a2} = 0$ if $a \neq 0$, and $t_{02} = q$. To determine t_{a1} we need an additional observation. We know that for every index $1 \leq v \leq \ell$, w acts like $\rho_{i_v}^s$ on C_{i_v}. In particular, by (5-3) we have $w(0, i_v) = (\bar{s}, i_v)$. However, by (5-2), $w(0, i_v) = (f(i_v), i_v)$. Thus $f(i_v) = \bar{s}$ for all v. Now, t_{a1} is the number of indices $1 \leq v \leq \ell$ such that $f(i_v) = a$. Clearly then, $t_{a1} = 0$ if $a \neq \bar{s}$ and $t_{\bar{s}1} = \ell$. This determines the type of w.

Proposition 5.2 yields

$$|\mathcal{C}| = \ell! q! n^\ell (2n)^q.$$

Let $w' = (\rho_1 \cdots \rho_\ell)^s \varepsilon$, where $\varepsilon = (\ell + 1, \ell + 2) \cdots (r - 1, r) \in S_r$. A straightforward calculation shows that w' has the same type as w, and is therefore conjugate to w. This completes the proof of 1(b).

We now prove 2(a). If w acts nontrivially on m of the sets C_i, then the number of elements moved by w is mn; hence $m = 2$, so w acts trivially on all but two of these sets, say C_i and C_j with $i < j$. By Lemma 5.3, there exist integers $0 < u, v < n$ such that w acts like ρ_i^u on C_i and like ρ_j^v on C_j. The w-orbit of every element of C_i then has size $n/\gcd(n, u) = 2$, so n is even and $u = n/2$. Similarly, $v = n/2$. Thus w acts like $(\rho_i \rho_j)^{n/2}$ on all of X, and therefore $w = (\rho_i \rho_j)^{n/2}$. Letting $s = n/2$, we have $w = (s\delta_i + s\delta_j, 1)$; the type of w is now easily determined.

We have $t_{ak} = 0$ if $k > 1$, and t_{a1} is the number of indices $k \in \Omega$ such that $s\delta_i(k) + s\delta_j(k) = a$. Now, note that

$$s\delta_i(k) + s\delta_j(k) = 0, \quad \text{if } k \neq i, j, \quad \text{and} \quad s\delta_i(k) + s\delta_j(k) = \bar{s}, \quad \text{if } k = i \text{ or } j.$$

Hence $t_{a1} = 0$ if $a \notin \{0, \bar{s}\}$, $t_{\bar{s}1} = 2$, and $t_{01} = r - 2$. Proposition 5.2 now yields $|\mathcal{C}| = 2(r - 2)! n^r$; this proves 2(a).

Next we prove 2(b). By Lemma 5.3 we have $w(C_i) = C_j$ for some $j \neq i$. Then $w(C_j)$ must equal C_i, for otherwise w would move more than $2n$ elements of X. Thus $w(C_i) = C_j$, $w(C_j) = C_i$, and w acts trivially on C_k for all $k \neq i, j$. It follows from Lemma 5.3 that $\pi = (i, j)$. Reversing the roles of i and j if

necessary, we may assume that $i < j$. By Lemma 5.4, there exists $0 \le s < n$ such that $w(\alpha) = \rho_i^{-s}\pi\rho_i^s(\alpha)$ for every $\alpha \in C_i \cup C_j$. Clearly, this equality also holds if $\alpha \in C_k$ with $k \notin \{i, j\}$, so $w = \rho_i^{-s}\pi\rho_i^s$. We can now determine the type of w.

Since w and $\pi = (i, j)$ are conjugate, they have the same type. We thus find that $t_{ak} = 0$ if $k > 2$; $t_{a2} = 0$ if $a \neq 0$, and $t_{02} = 1$; $t_{a1} = 0$ if $a \neq 0$, and $t_{01} = r - 2$. Proposition 5.2 now yields $|\mathcal{C}| = 2(r-2)!n^{r-1}$; this completes the proof of 2(b).

Finally, we prove (3). It is easy to see that the n elements moved by w must form one of the sets C_i. This implies that $w(C_i) = C_i$ and w acts trivially on C_j for all $j \neq i$. By Lemma 5.3, there exists $0 < s < n$ such that $w(\alpha) = \rho_i^s(\alpha)$ for every $\alpha \in C_i$. This equality clearly holds for $\alpha \notin C_i$ as well, so $w = \rho_i^s$. Using the relation $w = \rho_i^s = (s\delta_i, 1)$, it is now a simple calculation to show that $t_{ak} = 0$ if $k > 1$, $t_{a1} = 0$ if $a \notin \{0, \bar{s}\}$, $t_{\bar{s}1} = 1$, and $t_{01} = r - 1$. Proposition 5.2 now yields $|\mathcal{C}| = (r-1)!n^r$. □

Having developed all of the necessary tools, we proceed to prove the main results of this article.

6. Genus computations for $n = 5$ and 6

Recall the following notation from Section 4: $K = \overline{\mathbb{Q}}(t)$, N/K is a splitting field of Φ_n, $G = \mathrm{Gal}(N/K)$, F is a subfield of N obtained by adjoining one root of Φ_n to K, and $\mathbb{P} = \{p_\infty\} \cup \{p_b \mid b \in \bigcup_{d\,|\,n} R_{n,d}\}$ is the set of places of K that ramify in F. Finally, for any intermediate field L in the extension N/K and any place p of K, $\mathbb{P}_L(p)$ denotes the set of places of L lying over p.

We begin this section by discussing an approach to the problem of computing the genera of subextensions of N/K. Let H be a subgroup of G with fixed field L, and let $g(L)$ denote the genus of L. We claim that if p is a place of K which ramifies in L, then $p \in \mathbb{P}$. Indeed, if p ramifies in L, then it ramifies in N. Letting $\mathfrak{P}$ be a place of N lying over p, the inertia group $I_{\mathfrak{P}\,|\,p}$ is nontrivial, so Corollary 3.5 implies that p ramifies in F. Hence $p \in \mathbb{P}$.

The Hurwitz genus formula [Stichtenoth 2009, Corollary 3.5.6] now yields

$$2g(L) - 2 = (-2)|G : H| + \sum_{p \in \mathbb{P}} \sum_{\mathfrak{q} \in \mathbb{P}_L(p)} (e_{\mathfrak{q}\,|\,p} - 1). \tag{6-1}$$

Let us define

$$g_{n,\infty}(H) = \sum_{\mathfrak{q} \in \mathbb{P}_L(p_\infty)} (e_{\mathfrak{q}\,|\,p_\infty} - 1),$$

and for every divisor d of n,

$$g_{n,d}(H) = \sum_{b \in R_{n,d}} \sum_{\mathfrak{q} \in \mathbb{P}_L(p_b)} (e_{\mathfrak{q}\,|\,p_b} - 1).$$

By (6-1) we have the following expression for the genus of L:

$$g(L) = 1 - |G : H| + \tfrac{1}{2}\left(g_{n,\infty}(H) + \sum_{d\,|\,n} g_{n,d}(H)\right). \tag{6-2}$$

The problem of computing $g(L)$ is thus reduced to the following: given any place $p \in \mathbb{P}$, compute the ramification index $e_{\mathfrak{q}\,|\,p}$ for every $\mathfrak{q} \in \mathbb{P}_L(p)$. Our method for doing this is based on the following lemma.

Lemma 6.1. *Let $p \in \mathbb{P}$, $\mathfrak{P} \in \mathbb{P}_N(p)$, and $I = I_{\mathfrak{P}\,|\,p}$. Let $\sigma_1, \ldots, \sigma_m$ be representatives of the distinct double cosets in $I\backslash G/H$. Then*

$$\{e_{\mathfrak{q}\,|\,p} : \mathfrak{q} \in \mathbb{P}_L(p)\} = \{|I^{\sigma_i} : I^{\sigma_i} \cap H| : 1 \le i \le m\}.$$

Proof. Since K is a function field over $\overline{\mathbb{Q}}$, we have $f_{\mathfrak{P}\,|\,p} = 1$ and therefore $D_{\mathfrak{P}\,|\,p} = I_{\mathfrak{P}\,|\,p} = I$. Using Lemma 3.1 we see that the set $\mathbb{P}_L(p)$ consists of the places $\sigma_i(\mathfrak{P}) \cap L$; moreover, if $\mathfrak{q} = \sigma_i(\mathfrak{P}) \cap L$, then $e_{\mathfrak{q}\,|\,p} = |I^{\sigma_i} : I^{\sigma_i} \cap H|$. The result follows immediately. □

For purposes of explicit computation it is convenient to use the isomorphisms $G \equiv \mathcal{W} \equiv \mathcal{Z}$ proved in Sections 5B–5D. With notation as in Lemma 6.1, suppose that one is able to identify the subgroup of $\mathcal{W}$ (or $\mathcal{Z}$) which corresponds to the inertia group I. It is then a finite computation to determine representatives $\sigma_1, \ldots, \sigma_m$ and to compute the indices $|I^{\sigma_i} : I^{\sigma_i} \cap H|$. Carrying out this calculation for every $p \in \mathbb{P}$, one obtains all the data needed to determine the numbers $g_{n,\infty}$ and $g_{n,d}$, and hence the genus of L.

The remainder of this section is devoted to showing that when $n = 5$ or 6 it is possible — and computationally feasible — to identify inertia groups $I_{\mathfrak{P}\,|\,p}$ for every $p \in \mathbb{P}$, and thus to compute the genus of any intermediate field in the extension N/K. In particular, this allows us to obtain the genera of the fixed fields of all the maximal subgroup of G, and by applying Proposition 2.4, to show that the sets E_5 and E_6 are finite.

In order to carry out all the necessary computations we have used version 2.23-1 of MAGMA [Bosma et al. 1997] running on a MacBook Pro with a 2.7 GHz Intel Core i5 processor and 8 GB of memory. The interested reader can find the code for our computations in [Krumm 2018a]. The code relies primarily on four intrinsic MAGMA functions: `WreathProduct`, `MaximalSubgroups`, `DoubleCosetRepresentatives`, and `meet`. The first function applied to $\mathbb{Z}/n\mathbb{Z}$ and S_r constructs the group $\mathcal{W}$ together with the natural embeddings $S_r \hookrightarrow \mathcal{W}$ and $(\mathbb{Z}/n\mathbb{Z})^r \hookrightarrow \mathcal{W}$. (It should be noted, however, that internally $\mathcal{W}$ is constructed as the group $\mathcal{Z}$.) Once $\mathcal{W}$ is constructed, the second function can be used to obtain the maximal subgroups of $\mathcal{W}$ up to conjugacy; the algorithm used is described in [Cannon and Holt 2004]. Given subgroups I and H of $\mathcal{W}$, the third function computes representatives of the double cosets in $I\backslash\mathcal{W}/H$. Finally, the fourth function can be used to compute the intersection of two subgroups of $\mathcal{W}$; the algorithm uses a backtrack method described in [Leon 1997].

Throughout this section we use the following notation. For $1 \le i \le r$ we let ρ_i be the element of $\mathcal{W}$ defined in Section 5F. As an automorphism of the graph Γ, ρ_i is a $1/n$ rotation of the i-th cycle. As an element of the group $\mathcal{Z}$, ρ_i is the i-th cycle in the decomposition of the permutation σ defined in Section 5B. For distinct indices $1 \le i, j \le r$ we let $\tau_{i,j}$ be the transposition $(i, j) \in S_r$ regarded as an element of $\mathcal{W}$. As an automorphism of Γ, $\tau_{i,j}$ interchanges the i-th and j-th cycles without performing any rotations.

Lemma 6.2. *The elements $\rho_1, \ldots, \rho_r$ are conjugate in $\mathcal{W}$. Moreover, if $i, j, u, v \in \{1, \ldots, r\}$ with $i \ne j$ and $u \ne v$, then $\rho_i\rho_j$ is conjugate to $\rho_u\rho_v$.*

Proof. This follows from Proposition 5.2. The type (t_{ak}) of ρ_i is independent of i; indeed, we have $t_{ak} = 0$ if $k > 1$, $t_{a1} = 0$ if $a \neq 0, 1$, $t_{01} = r - 1$, and $t_{11} = 1$. Similarly, if $i \neq j$, then the type (t_{ak}) of $\rho_i \rho_j$ independent of i and j: we have $t_{ak} = 0$ if $k > 1$, $t_{a1} = 0$ if $a \neq 0, 1$, $t_{01} = r - 2$, and $t_{11} = 2$. □

6A. ***The case n = 5.*** The polynomial Φ_5 has $D = 2\nu(5) = 30$ roots which can be partitioned into $r = D/5 = 6$ cycles. Hence, the graph Γ consists of six 5-cycles. The group $\mathcal{W}$ is $(\mathbb{Z}/5\mathbb{Z}) \wr S_6$, so $|G| = 5^6 6! = 11{,}250{,}000$. The set of places of K which ramify in F is

$$\mathbb{P} = \{p_\infty\} \cup \{p_b \mid b \in R_{5,5} \cup R_{5,1}\};$$

using Lemma 4.1 we obtain $\#R_{5,5} = 11$ and $\#R_{5,1} = 4$. We will henceforth identify G and $\mathcal{W}$ using the isomorphism $G \equiv \mathcal{W}$, where G acts on the roots of Φ_5 and $\mathcal{W}$ acts on the set $X = (\mathbb{Z}/5\mathbb{Z}) \times \{1, \ldots, 6\}$.

We define three subgroups of $\mathcal{W}$ by $A = \langle \tau_{1,2}\tau_{3,4}\tau_{5,6} \rangle$, $B = \langle \tau_{1,2} \rangle$, $C = \langle \rho_1 \rangle$.

Lemma 6.3. *Up to conjugation, A is the only subgroup of $\mathcal{W}$ generated by an element with cycle type* $(2, 15)$; *similarly, B is uniquely determined by the cycle type* $(2, 5)$, *and C by the cycle type* $(5, 1)$.

Proof. Suppose that $\tilde{A}$ is a subgroup of $\mathcal{W}$ generated by an element w with cycle type $(2, 15)$. We are then in the context of case 1 of Proposition 5.5. Moreover, since $n = 5$ is odd, case 1(b) is ruled out. Hence, by case 1(a), w is conjugate to $\tau_{1,2}\tau_{3,4}\tau_{5,6}$, and therefore $\tilde{A}$ is conjugate to A.

Now suppose that a subgroup $\tilde{B}$ is generated by an element w with cycle type $(2, 5)$. By case 2(b) of Proposition 5.5, w is conjugate to $\tau_{i,j}$ for some indices i, j. Clearly the permutations (i, j) and $(1, 2)$ are conjugates in S_6, so $\tau_{i,j}$ is conjugate to $\tau_{1,2}$ and therefore $\tilde{B}$ is conjugate to B.

Finally, suppose that a subgroup $\tilde{C}$ is generated by an element w with cycle type $(5, 1)$. By case 3 of Proposition 5.5, we have $w = \rho_i^s$ for some i and $0 < s < 5$. Note that $\langle \rho_i^s \rangle = \langle \rho_i \rangle$ since $|\rho_i| = 5$. By Lemma 6.2, w is conjugate to ρ_1^s, and therefore $\tilde{C} = \langle w \rangle$ is conjugate to $\langle \rho_1^s \rangle = \langle \rho_1 \rangle = C$. □

Lemma 6.4. (1) *There exists $\mathfrak{P} \in \mathbb{P}_N(p_\infty)$ such that $I_{\mathfrak{P}\,|\,p_\infty} = A$.*

(2) *For every $b \in R_{5,5}$ there exists $\mathfrak{P} \in \mathbb{P}_N(p_b)$ such that $I_{\mathfrak{P}\,|\,p_b} = B$.*

(3) *For every $b \in R_{5,1}$ there exists $\mathfrak{P} \in \mathbb{P}_N(p_b)$ such that $I_{\mathfrak{P}\,|\,p_b} = C$.*

Proof. Let $\mathfrak{P} \in \mathbb{P}_N(p_\infty)$. By Proposition 4.3 we have $I_{\mathfrak{P}\,|\,p_\infty} = \langle w \rangle$, where $w \in \mathcal{W}$ has cycle type $(2, 15)$. Thus, by Lemma 6.3, $I_{\mathfrak{P}\,|\,p_\infty}$ is conjugate to A. Replacing $\mathfrak{P}$ by a conjugate place if necessary, we then have $I_{\mathfrak{P}\,|\,p_\infty} = A$. This proves (1); the proofs of (2) and (3) are similar. □

Proposition 6.5. *Let H be a subgroup of $\mathcal{W}$ with fixed field L. Suppose that $\alpha_1, \ldots, \alpha_t$ are double coset representatives for $A\backslash\mathcal{W}/H$, $\beta_1, \ldots, \beta_u$ are representatives for $B\backslash\mathcal{W}/H$, and $\gamma_1, \ldots, \gamma_v$ are representatives for $C\backslash\mathcal{W}/H$. Then the genus of L is given by*

$$g(L) = 1 - |\mathcal{W} : H| + \tfrac{1}{2}(g_{5,\infty}(H) + g_{5,5}(H) + g_{5,1}(H)),$$

where

$$g_{5,\infty}(H) = \sum_{i=1}^{t} (|A^{\alpha_i} : A^{\alpha_i} \cap H| - 1), \tag{6-3}$$

$$g_{5,5}(H) = 11 \cdot \sum_{i=1}^{u} (|B^{\beta_i} : B^{\beta_i} \cap H| - 1), \tag{6-4}$$

$$g_{5,1}(H) = 4 \cdot \sum_{i=1}^{v} (|C^{\gamma_i} : C^{\gamma_i} \cap H| - 1). \tag{6-5}$$

Proof. The formula for $g(L)$ follows from (6-2). Let $p = p_\infty$. By Lemma 6.4, there exists $\mathfrak{P} \in \mathbb{P}_N(p)$ such that $I_{\mathfrak{P}\,|\,p} = A$. By Lemma 6.1 we have

$$\{e_{\mathfrak{q}\,|\,p} : \mathfrak{q} \in \mathbb{P}_L(p)\} = \{|A^{\alpha_i} : A^{\alpha_i} \cap H| : 1 \le i \le t\},$$

which implies (6-3). Now suppose that $b \in R_{5,5}$ and let $p = p_b$. By Lemma 6.4, there exists $\mathfrak{P} \in \mathbb{P}_N(p)$ such that $I_{\mathfrak{P}\,|\,p} = B$. Thus, by Lemma 6.1,

$$\{e_{\mathfrak{q}\,|\,p} : \mathfrak{q} \in \mathbb{P}_L(p)\} = \{|B^{\beta_i} : B^{\beta_i} \cap H| : 1 \le i \le u\},$$

and therefore

$$\sum_{\mathfrak{q} \in \mathbb{P}_L(p)} (e_{\mathfrak{q}\,|\,p} - 1) = \sum_{i=1}^{u} (|B^{\beta_i} : B^{\beta_i} \cap H| - 1).$$

Since the value of this sum is independent of b, and $\#R_{5,5} = 11$, then

$$g_{5,5}(H) = \sum_{b \in R_{5,5}} \sum_{\mathfrak{q} \in \mathbb{P}_L(p_b)} (e_{\mathfrak{q}\,|\,p_b} - 1) = 11 \cdot \sum_{i=1}^{u} (|B^{\beta_i} : B^{\beta_i} \cap H| - 1),$$

which proves (6-4). The proof of (6-5) is similar. □

We can now begin to prove Theorem 1.4.

Theorem 6.6. *The set E_5 is finite.*

Proof. Computing representatives for the conjugacy classes of maximal subgroups of $\mathcal{W}$, we obtain 8 subgroups which we denote by $M_1, \ldots, M_8$. The indices of these subgroups in $\mathcal{W}$ are given, respectively, by

$$|\mathcal{W} : M_i| : 3125, 15, 15, 10, 6, 6, 5, 2.$$

Let L_i be the fixed field of M_i. Fixing an index i, we may compute representatives for the double cosets in $A\backslash\mathcal{W}/M_i$, $B\backslash\mathcal{W}/M_i$, and $C\backslash\mathcal{W}/M_i$. The genus of L_i can then be obtained by applying Proposition 6.5. Carrying out these computations for $i = 1, \ldots, 8$ we obtain, respectively, the genera

$$9526, 21, 11, 9, 2, 12, 4, 5.$$

	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
$g_{5,\infty}$	1550	4	6	3	3	1	0	1
$g_{5,5}$	13750	66	44	33	11	33	0	11
$g_{5,1}$	10000	0	0	0	0	0	16	0

Table 1. Ramification data for the maximal subgroups of $\mathcal{W}$.

The result now follows from Proposition 2.4. The values of $g_{5,\infty}(M_i)$, $g_{5,5}(M_i)$, and $g_{5,1}(M_i)$ are shown in Table 1. □

6B. ***The case n = 6.*** Our next objective is to show that the set E_6 is finite. The structure of the proof is similar to the case $n = 5$, though the process of identifying the necessary inertia groups requires an additional step that was not present in that case.

The polynomial Φ_6 has $D = 2\nu(6) = 54$ roots which can be partitioned into $r = D/6 = 9$ cycles. Hence, the graph Γ consists of nine 6-cycles. The group $\mathcal{W}$ is $(\mathbb{Z}/6\mathbb{Z}) \wr S_9$, so $|G| = 6^9 9! = 3{,}656{,}994{,}324{,}480$. The set of places of K which ramify in F is $\mathbb{P} = \{p_\infty\} \cup \left\{p_b \mid b \in \bigcup_{d\,|\,6} R_{6,d}\right\}$. Using Lemma 4.1 we find that

$$\#R_{6,6} = 20, \quad \#R_{6,3} = 3, \quad \#R_{6,2} = 2, \quad \#R_{6,1} = 2. \tag{6-6}$$

We define several cyclic subgroups of $\mathcal{W}$. For $0 \le j \le 4$, let

$$\gamma_j = \left(\prod_{i=1}^{9-2j} \rho_i^3\right)\left(\prod_{i=0}^{j-1} \tau_{8-2i,9-2i}\right) \quad \text{and} \quad A_j = \langle \gamma_j \rangle.$$

In addition, let $B_0 = \langle \rho_1^3 \rho_2^3 \rangle$, $B_1 = \langle \tau_{1,2} \rangle$, $C = \langle \rho_1^3 \rangle$, $D = \langle \rho_1^2 \rangle$, $E = \langle \rho_1 \rangle$.

Lemma 6.7. *Up to conjugation, the groups A_j are the only subgroups of $\mathcal{W}$ generated by an element with cycle type* $(2, 27)$, *B_0 and B_1 are the only subgroups generated by an element with cycle type* $(2, 6)$, *and C, D, E are uniquely determined by the cycle types* $(2, 3)$, $(3, 2)$, *and* $(6, 1)$, *respectively.*

Proof. Suppose that $\tilde{A} = \langle w \rangle$, where $w \in \mathcal{W}$ has cycle type $(2, 27)$. We are then in the context of case 1 of Proposition 5.5. Moreover, since $r = 9$ is odd, case 1(b) must hold. Thus, there exists $0 < \ell \le 9$ such that $9 - \ell$ is even and w is conjugate to $v = (\rho_1 \cdots \rho_\ell)^3 (\tau_{\ell+1,\ell+2}) \cdots \tau_{8,9}$. Writing $9 - \ell = 2j$ with $0 \le j \le 4$, we have $v = \gamma_j$. Hence, $\tilde{A}$ is conjugate to A_j.

Suppose now that $\tilde{B} = \langle w \rangle$, where $w \in \mathcal{W}$ has cycle type $(2, 6)$. We are then in the context of case 2 of Proposition 5.5. In case 2(a) of the proposition, $w = (\rho_i \rho_j)^3$ for some indices $i \ne j$. By Lemma 6.2, this implies that w is conjugate to $(\rho_1 \rho_2)^3$, and therefore $\tilde{B}$ is conjugate to B_0. In case 2(b) of the proposition, w is conjugate to $\tau_{1,2}$ and $\tilde{B}$ is conjugate to B_1.

We now prove the uniqueness of the group C and omit the proofs for D and E, which are similar. Suppose that $\tilde{C} = \langle w \rangle$, where $w \in \mathcal{W}$ has cycle type $(2, 3)$. By case (3) of Proposition 5.5, we have $w = \rho_i^s$ with $1 \le i \le 9$ and $0 < s < 6$. In order for w to have cycle type $(2, 3)$ we must have $s = 3$; thus, by Lemma 6.2, w is conjugate to ρ_1^3 and $\tilde{C}$ is conjugate to C. □

Before continuing with the main discussion of this section, we prove a couple of auxiliary results. Returning to the general case of an arbitrary positive integer n, let θ be a root of Φ_n such that $F = K(\theta)$. Recall from Section 4 that F has an automorphism given by $\theta \mapsto \phi(\theta)$, and that F_0 denotes the fixed field of this automorphism.

Lemma 6.8. *Let* $\tau = \theta + \phi(\theta) + \cdots + \phi^{n-1}(\theta)$. *Then* $F_0 = K(\tau)$.

Proof. Following Morton [1996], we define the *trace* of a cycle in the graph Γ to be the sum of the elements in the cycle. Note that τ is the trace of the cycle containing θ. Let $P \in K[x]$ be the monic polynomial of degree r whose roots are the traces of all the cycles in Γ. By [Morton 1996, Corollary 3, p. 335], P is irreducible; hence P is the minimal polynomial of τ, and therefore $[K(\tau) : K] = r$. Clearly τ is fixed by ϕ, so $K(\tau) \subseteq F_0$. Now, since $[F : K] = D$ and $[F : F_0] = n$, then $[F_0 : K] = D/n = r = [K(\tau) : K]$. Thus $F_0 = K(\tau)$. □

We can now describe the subgroup of G corresponding to F_0.

Lemma 6.9. *Let* $\mathcal{O} = \{\theta, \phi(\theta), \ldots, \phi^{n-1}(\theta)\}$ *and let* H_0 *be the setwise stabilizer of* $\mathcal{O}$ *in* G. *Then* F_0 *is the fixed field of* H_0.

Proof. Let U and V be the subgroups of G defined by

$$U = \{\sigma \in G \mid \sigma(x) = x \text{ for every } x \in \mathcal{O}\} \quad \text{and} \quad V = \{\sigma \in G \mid \sigma(x) = x \text{ for every } x \in R \setminus \mathcal{O}\}.$$

A simple argument shows that $H_0 = UV$; see Example 2 in [Dummit and Foote 2004, p. 172].

The fact that ϕ is in the center of G implies that U is equal to the stabilizer of θ in G; thus $U = \mathrm{Gal}(N/F)$. It follows that F is the fixed field of U. Let L be the fixed field of H_0. Since $U \leq H_0$, then $L \subseteq F$. Defining τ as in Lemma 6.8, it is clear that τ is fixed by every element of H_0; hence $F_0 = K(\tau) \subseteq L$. We have thus shown that $F_0 \subseteq L \subseteq F$. To complete the proof we will show that $[F : L] = [F : F_0]$.

Identifying G with $\mathrm{Aut}(\Gamma)$ we see that V consists of the elements of G that act trivially on every cycle of Γ except possibly on the cycle containing θ. Thus the elements of V are the n rotations of the latter cycle, so $|V| = n$. By Galois theory we have $[F : L] = |UV|/|U| = |V|$, where the second equality uses the fact that $U \cap V = \{1\}$. We conclude that $[F : L] = n = [F : F_0]$. □

We return now to the case $n = 6$.

Lemma 6.10. (1) *There exists* $\mathfrak{P} \in \mathbb{P}_N(p_\infty)$ *such that* $I_{\mathfrak{P} \mid p_\infty} = A_4$.

(2) *For every* $b \in R_{6,6}$ *there exists* $\mathfrak{P} \in \mathbb{P}_N(p_b)$ *such that* $I_{\mathfrak{P} \mid p_b} = B_1$.

(3) *For every* $b \in R_{6,3}$ *there exists* $\mathfrak{P} \in \mathbb{P}_N(p_b)$ *such that* $I_{\mathfrak{P} \mid p_b} = C$.

(4) *For every* $b \in R_{6,2}$ *there exists* $\mathfrak{P} \in \mathbb{P}_N(p_b)$ *such that* $I_{\mathfrak{P} \mid p_b} = D$.

(5) *For every* $b \in R_{6,1}$ *there exists* $\mathfrak{P} \in \mathbb{P}_N(p_b)$ *such that* $I_{\mathfrak{P} \mid p_b} = E$.

Proof. Let $p = p_\infty$, $\mathfrak{P} \in \mathbb{P}_N(p)$, and $I = I_{\mathfrak{P} \mid p}$. By Proposition 4.3, I has a generator with cycle type $(2, 27)$. By Lemma 6.7, I must be conjugate to one of the groups A_j. Replacing $\mathfrak{P}$ by a conjugate ideal if necessary, we then have $I = A_j$ for some j. We claim that $I = A_4$.

To prove this we will use the number $S(p)$ defined in Proposition 4.4. By part (a) of the proposition, $S(p) = 9 - e_6 = 4$. We can calculate $S(p)$ in a different way by using the inertia group I as follows. Let H_0 be the subgroup of $\mathcal{W}$ defined in Lemma 6.9. Applying Lemma 6.1 we see that

$$S(p) = \sum_{i=1}^{m} (|I^{\sigma_i} : I^{\sigma_i} \cap H_0| - 1),$$

where $\sigma_1, \ldots, \sigma_m$ are double coset representatives for $I\backslash\mathcal{W}/H_0$. Assuming that $I = A_0, A_1, A_2, A_3, A_4$, respectively, we compute representatives σ_i and use the above formula to obtain $S(p) = 0, 1, 2, 3, 4$. However, we know that $S(p) = 4$, so necessarily $I = A_4$, as claimed. This proves (1). For the purposes of this computation, we identify $\mathcal{W}$ with the group $\mathcal{Z} \leq S_{54}$, so that H_0 is identified with the setwise stabilizer of the set $\{1, \ldots, 6\}$ in $\mathcal{Z}$. The code used for these computations is available in [Krumm 2018a].

Let $b \in R_{6,6}$, $p = p_b$, $\mathfrak{P} \in \mathbb{P}_N(p)$, and $I = I_{\mathfrak{P}\,|\,p}$. By Proposition 4.3, I has a generator with cycle type $(2, 6)$. By Lemma 6.7, I must be conjugate to either B_0 or B_1. Replacing $\mathfrak{P}$ by a conjugate ideal if necessary, we then have $I = B_0$ or B_1. We know that $S(p) = 1$ by part (b) of Proposition 4.4. Now, assuming that $I = B_0, B_1$, respectively, the above displayed formula yields $S(p) = 0, 1$; hence $I = B_1$. This proves (2).

Statements (3)-(5) follow easily from Proposition 4.3 and Lemma 6.7. □

Proposition 6.11. *Let H be a subgroup of $\mathcal{W}$ with fixed field L. For every group $I \in \{A_4, B_1, C, D, E\}$ let*

$$q_H(I) = \sum_{i=1}^{m} (|I^{\sigma_i} : I^{\sigma_i} \cap H| - 1),$$

where $\sigma_1, \ldots, \sigma_m$ are representatives of all the double cosets in $I\backslash\mathcal{W}/H$. Then the genus of L is given by

$$g(L) = 1 - |\mathcal{W} : H| + \tfrac{1}{2}(q_H(A_4) + 20q_H(B_1) + 3q_H(C) + 2q_H(D) + 2q_H(E)).$$

Proof. Let $p = p_\infty$. By Lemma 6.10, there exists $\mathfrak{P} \in \mathbb{P}_N(p)$ such that $I_{\mathfrak{P}\,|\,p} = A_4$. Using Lemma 6.1 we see that $g_{6,\infty}(H) = q_H(A_4)$. Now let $b \in R_{6,6}$, $p = p_b$, and let $\mathfrak{P} \in \mathbb{P}_N(p)$ satisfy $I_{\mathfrak{P}\,|\,p} = B_1$. By Lemma 6.1,

$$q_H(B_1) = \sum_{\mathfrak{q} \in \mathbb{P}_L(p)} (e_{\mathfrak{q}\,|\,p} - 1).$$

Since this holds for every $b \in R_{6,6}$, then (6-6) yields $g_{6,6}(H) = 20q_H(B_1)$. By a similar argument we show that

$$g_{6,3}(H) = 3q_H(C), \quad g_{6,2}(H) = 2q_H(D), \quad \text{and} \quad g_{6,1}(H) = 2q_H(E).$$

The stated formula for the genus of L is now a consequence of (6-1). □

We can now prove a second part of Theorem 1.4.

Theorem 6.12. *The set E_6 is finite.*

	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}
$q_{M_i}(A_4)$	416	132	120	60	40	16	4	0	1	0	1
$q_{M_i}(B_1)$	420	105	64	35	21	7	1	0	1	1	0
$q_{M_i}(C)$	0	0	128	0	0	0	0	0	1	0	1
$q_{M_i}(D)$	0	0	0	0	0	0	0	2	0	0	0
$q_{M_i}(E)$	0	0	128	0	0	0	0	2	1	0	1

Table 2. Ramification data for the maximal subgroups of $\mathcal{W}$.

Proof. Computing representatives for the conjugacy classes of maximal subgroups of $\mathcal{W}$, we obtain 11 subgroups which we denote by $M_1, \ldots, M_{11}$. The indices of these subgroups in $\mathcal{W}$ are given, respectively, by

$$|\mathcal{W} : M_i| : 840, 280, 256, 126, 84, 36, 9, 3, 2, 2, 2.$$

Let L_i be the fixed field of M_i. Fixing an index i, we may compute the numbers $q_{M_i}(I)$ for $I \in \{A_4, B_1, C, D, E\}$. The genus of L_i can then be obtained by applying Proposition 6.11. Carrying out these computations for $i = 1, \ldots, 11$ we obtain, respectively, the genera

$$3569, 837, 765, 255, 147, 43, 4, 2, 12, 9, 2.$$

By Proposition 2.4, this implies that E_6 is finite. The values of $q_{M_i}(I)$ are shown in Table 2. □

7. Genus bounds for $n > 6$

The methods used in the previous section for $n = 5$ and 6 can, in principle, be applied to higher values of n; however, there are computational limitations which make this impractical. Firstly, for $n > 10$ there are issues of both memory and time which prevent us from computing the maximal subgroups of $\mathcal{W}$. Thus, we are restricted to considering only $n = 7, 8, 9, 10$. Furthermore, even for these values of n there are similar complications in the crucial step of computing double coset representatives. Hence, it would appear that our methods cannot be extended beyond $n = 6$. However, a modification of the method will allow us to show that E_7 and E_9 are finite.

Recall that our main goal is to show that the genera of the function fields corresponding to maximal subgroups of G are all greater than 1. In the cases $n = 5, 6$ we did this by calculating the exact values of these genera, although it would be sufficient to prove a lower bound greater than 1. In this section we will show that, as long as the maximal subgroups of $\mathcal{W}$ can be computed, it is possible to obtain lower bounds for the required genera. In the cases $n = 7, 9$ these bounds will suffice to prove the desired result. Unfortunately, the bounds are not good enough when $n = 8, 10$; the difficulties are explained in Section 7B. We keep here all of the notation introduced in earlier sections.

Lemma 7.1. *Let H be a subgroup of G with fixed field L, and $a = |G : H|$. Let p be a place of K, let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\} = \mathbb{P}_L(p)$, and $e_i = e_{\mathfrak{q}_i \mid p}$. Suppose that u is an upper bound for the number of indices i such*

that $e_i = 1$. *Then*

$$\sum_{i=1}^{s}(e_i - 1) \geq \lceil a - \lfloor (u+a)/2 \rfloor \rceil.$$

Proof. Let x be the number of indices i such that $e_i = 1$, and let $y = s - x$. Note that $a = e_1 + \cdots + e_s \geq x + 2y$. Since $x \leq u$, this implies $x + y \leq (u+a)/2$. Thus $s \leq \lfloor (u+a)/2 \rfloor$ and therefore

$$\sum_{i=1}^{s}(e_i - 1) = a - s \geq a - \lfloor (u+a)/2 \rfloor,$$

from which the result follows immediately. □

7A. ***The case of odd n.*** Assume that n is odd. Using Lemma 7.1, we now explain how to obtain lower bounds for the genera of subextensions of N/K. Define subsets Θ_n and Λ_n of $\mathcal{W}$ by

$$\Theta_n = \{\rho_i^s \mid 1 \leq i \leq r, 0 < s < n\}, \quad \text{and} \quad \Lambda_n = \{\rho_i^{-s}\tau_{i,j}\rho_i^s \mid 1 \leq i < j \leq r, 0 \leq s < n\}.$$

For every subgroup H of $\mathcal{W}$ and every divisor d of n, let

$$u_{n,d}(H) = \begin{cases} (r-1)!n^r \#(H \cap \Theta_{n,d})/|H| & \text{if } d < n, \\ 2(r-2)!n^{r-1}\#(H \cap \Lambda_n)/|H| & \text{if } d = n, \end{cases}$$

and

$$g'_{n,d}(H) = (\deg \Delta_{n,d})\left\lceil |\mathcal{W} : H| - \left\lfloor \frac{u_{n,d}(H) + |\mathcal{W} : H|}{2} \right\rfloor \right\rceil.$$

Here, $\Theta_{n,d}$ denotes the set of elements of Θ_n having cycle type $(n/d, d)$.

Proposition 7.2. *With notation as above, let* L *be the fixed field of* H. *Then the genus of* L *satisfies*

$$g(L) \geq \left\lceil 1 - |\mathcal{W} : H| + \tfrac{1}{2}\sum_{d \mid n} \max(g'_{n,d}(H), 0) \right\rceil. \tag{7-1}$$

Proof. Let d be a proper divisor of n, and let $b \in R_{n,d}$. If $\mathfrak{P}$ is a place of N lying over p_b, Proposition 4.3 implies that the inertia group $I_{\mathfrak{P} \mid p_b}$ is generated by an element γ with cycle type $(n/d, d)$. By part (3) of Proposition 5.5, we have $\gamma = \rho_i^s$ with $1 \leq i \leq r$ and $0 < s < n$. Moreover, the order of the centralizer of γ is given by $|C_{\mathcal{W}}(\gamma)| = (r-1)!n^r$. Thus, by Corollary 3.5, the number of places $\mathfrak{q} \in \mathbb{P}_L(p_b)$ such that $e_{\mathfrak{q} \mid p_b} = 1$ is equal to

$$(r-1)!n^r s(H, \gamma)/|H|,$$

where $s(H, \gamma)$ is the number of conjugates of γ which belong to H. Note that every conjugate of γ belongs to $\Theta_{n,d}$, so that $s(H, \gamma) \leq \#(H \cap \Theta_{n,d})$. It follows that the number of places $\mathfrak{q} \in \mathbb{P}_L(p_b)$ such that $e_{\mathfrak{q} \mid p_b} = 1$ is bounded above by $u_{n,d}(H)$. Letting $a = |\mathcal{W} : H|$, Lemma 7.1 implies that

$$\sum_{\mathfrak{q} \in \mathbb{P}_L(p_b)} (e_{\mathfrak{q} \mid p_b} - 1) \geq \lceil a - \lfloor (u_{n,d}(H) + a)/2 \rfloor \rceil.$$

Recalling the number $g_{n,d}(H)$ defined in Section 6, the above inequality implies that $g_{n,d}(H) \geq g'_{n,d}(H)$ and therefore $g_{n,d}(H) \geq \max(g'_{n,d}(H), 0)$.

By a similar argument we can show that $g_{n,n}(H) \geq \max(g'_{n,n}(H), 0)$. Let $b \in R_{n,n}$ and $\mathfrak{P} \in \mathbb{P}_N(p_b)$. Then $I_{\mathfrak{P}\,|\,p_b} = \langle \gamma \rangle$, where γ has cycle type $(2, n)$. Since n is odd, part 2(b) of Proposition 5.5 implies that $\gamma = \rho_i^{-s} \tau_{i,j} \rho_i^s$ for some $1 \leq i < j \leq r$ and $0 \leq s < n$. Moreover, $|C_{\mathcal{W}}(\gamma)| = 2(r-2)!n^{r-1}$. The number of places $\mathfrak{q} \in \mathbb{P}_L(p_b)$ such that $e_{\mathfrak{q}\,|\,p_b} = 1$ is therefore given by

$$2(r-2)!n^{r-1} s(H, \gamma)/|H|.$$

Now, every conjugate of γ belongs to Λ_n, so $s(H, \gamma) \leq \#(H \cap \Lambda_n)$. The number of places $\mathfrak{q} \in \mathbb{P}_L(p_b)$ with $e_{\mathfrak{q}\,|\,p_b} = 1$ is thus bounded above by $u_{n,n}$. Letting $a = |\mathcal{W} : H|$, we have

$$\sum_{\mathfrak{q} \in \mathbb{P}_L(p_b)} (e_{\mathfrak{q}\,|\,p_b} - 1) \geq \left\lceil a - \lfloor (u_{n,n}(H) + a)/2 \rfloor \right\rceil,$$

which implies that $g_{n,n}(H) \geq g'_{n,n}(H)$. We have thus proved:

$$g_{n,d}(H) \geq \max(g'_{n,d}(H), 0), \quad \text{for every divisor } d \text{ of } n.$$

Now (7-1) follows from the genus formula (6-2). □

Remark 7.3. Note that in proving the bound (7-1) we have disregarded the contribution to the genus coming from ramified places lying over p_∞. Though the bound would certainly be improved if these places were considered, doing so would substantially increase the amount of time and memory required to compute the bound. In particular, it would require determining the intersection $H \cap C$, where C is the set of all conjugates in $\mathcal{W}$ of the permutation $(1, 2)(3, 4) \cdots (r-1, r)$. Now, part 1(a) of Proposition 5.5 implies that $\#C = (n^r r!)/((r/2)!(2n)^{r/2}) \geq n^{r/2}$, which suggests that C might be difficult to construct in practice. And indeed, our attempts to compute all the elements of C in the case $n = 7$ failed due to excessive memory requirements.

Remark 7.4. In order to compute the number on the right-hand side of (7-1), the key step is to determine the cardinalities of the sets $H \cap \Theta_{n,d}$ and $H \cap \Lambda_n$, which would be difficult to do if all the sets involved were quite large. Fortunately, while the group H may be extremely large (for instance, H might be the largest maximal subgroup of the Galois group of Φ_9, in which case $|H| \approx 9.73 \times 10^{127}$), the sets Λ_n and $\Theta_{n,d}$ are small. Indeed, $\#\Theta_{n,d} \leq \#\Theta_n = r(n-1)$ and $\#\Lambda_n = n \cdot \binom{r}{2}$. This makes it computationally feasible to construct the sets $H \cap \Lambda_n$ and $H \cap \Theta_{n,d}$, and hence to compute the desired lower bound.

We can now complete the proof of Theorem 1.4. The finiteness of E_7 and E_9 is proved by a series of computations carried out using MAGMA; the code used for these computations is available in [Krumm 2018a].

Theorem 7.5. *The sets E_7 and E_9 are finite.*

Proof. We consider first the case of E_7. The polynomial Φ_7 has $D = 126$ roots which can be partitioned into $r = 18$ cycles. Thus, $\mathcal{W} = (\mathbb{Z}/7\mathbb{Z}) \wr S_{18}$. Constructing the group $\mathcal{W}$ and computing representatives for

the conjugacy classes of maximal subgroups of $\mathcal{W}$, we obtain 16 groups which we denote by $M_1, \ldots, M_{16}$. The sets Θ_7 and Λ_7 are easily constructed; we find that $\#\Theta_7 = 108$ and $\#\Lambda_7 = 1071$.

Let L_i denote the fixed field of M_i. For each subgroup M_i we compute the numbers $u_{7,7}(M_i)$ and $u_{7,1}(M_i)$, and use these to calculate $g'_{7,7}(M_i)$ and $g'_{7,1}(M_i)$. This is a trivial computation given the small size of the sets Θ_7 and Λ_7. The inequality (7-1) then yields a lower bound for $g(L_i)$.

Carrying out these calculations, the lowest lower bound we obtain for the genera $g(L_i)$ is 6; hence $g(L_i) > 1$ for every i, which implies that E_7 is finite. The total time required for all of the above computations is 0.42 s.

The proof of finiteness of E_9 follows the same steps as above. In this case the lowest lower bound we obtain for $g(L_i)$ is 4. Total computation time is 197 s, with 179 s spent computing the maximal subgroups of $\mathcal{W}$. □

7B. ***The case of even n.*** In the case where n is even, a bound similar to (7-1) can be proved; indeed, this only requires modifying the definition of the number $u_{n,n}(H)$. Unfortunately, when $n = 8$ or 10 the bounds for the genera $g(L_i)$ obtained in this way are not greater than 1; in fact many of them are negative. We suspect, therefore, that most of the ramification in the extensions L_i/K occurs over the place p_∞. In order to improve the bounds for $g(L_i)$ we would have to determine the genus contribution coming from places lying over p_∞. However, as discussed in Remark 7.3, it is computationally infeasible to do this. Thus, we are unable to improve the bounds enough to show that E_8 and E_{10} are finite.

8. Density results

Having proved Theorem 1.4, we now turn our attention to Theorem 1.5. Recall that if n is a positive integer and $c \in \mathbb{Q}$, we denote by $T_{n,c}$ the set of prime numbers p such that the map $\phi_c(x) = x^2 + c$ does not have a point of period n in $\mathbb{Q}_p$. By applying Lemma 8.1 below we will be able to calculate the density of $T_{n,c}$ for $n \in \{5, 6, 7, 9\}$ and all but finitely many $c \in \mathbb{Q}$.

For every polynomial $F \in \mathbb{Q}[x]$, let S_F be the set of all primes p such that F has a root in $\mathbb{Q}_p$. The Chebotarev density theorem implies that the density of S_F, which we denote by $\delta(S_F)$, exists and can be computed if the Galois group of F is known. More precisely, we have the following result.

Lemma 8.1. *Let $F \in \mathbb{Q}[x]$ be a separable polynomial of degree $D \geq 1$. Let S be a splitting field for F, and set $G = \mathrm{Gal}(S/\mathbb{Q})$. Let $\alpha_1, \ldots, \alpha_D$ be the roots of F in S and, for each index i, let G_i denote the stabilizer of α_i under the action of G. Then the Dirichlet density of S_F is given by*

$$\delta(S_F) = \frac{\left|\bigcup_{i=1}^{D} G_i\right|}{|G|}. \tag{8-1}$$

Proof. This follows from Theorem 2.1 in [Krumm 2016]. □

Note that for the purpose of computing $\delta(S_F)$ using the formula (8-1), the group G may be replaced with any permutation group $\mathcal{G}$ such that $G \equiv \mathcal{G}$. Fixing a positive integer n, let G_n be the Galois group of Φ_n over $\mathbb{Q}(t)$ and let $\mathcal{G} = \mathrm{Aut}(\Gamma)$, where Γ is the graph defined in Section 5A. Recall that $G_n \equiv \mathcal{G}$.

Lemma 8.2. *Let $\mathcal{M}$ be the set of all elements of $\mathcal{G}$ having no fixed point. The cardinality of $\mathcal{M}$ is given by the formula*

$$\#\mathcal{M} = \sum_{i=0}^{r} (n-1)^i \cdot n^{r-i} \cdot d(r,i),$$

where

$$d(r,i) = \binom{r}{i}(r-i)! \sum_{k=0}^{r-i} \frac{(-1)^k}{k!}.$$

Proof. The number $d(r,i)$ counts the permutations in S_r which fix exactly i elements of the set $\{1,\dots,r\}$. The above formula for $d(r,i)$ is proved by an inclusion-exclusion argument; see Example 2.2.1 in [Stanley 2012].

For $0 \le i \le r$, let $\mathcal{M}_i$ be the set of elements of $\mathcal{M}$ which fix exactly i cycles of Γ. Clearly $\mathcal{M}$ is a disjoint union of the sets $\mathcal{M}_i$, so in order to prove the lemma it suffices to show that

$$\#\mathcal{M}_i = (n-1)^i \cdot n^{r-i} \cdot d(r,i).$$

Recall that every element $\sigma \in \mathcal{G}$ has a unique representation of the form $\rho_1^{a_1} \cdots \rho_r^{a_r} \pi$, where $\pi \in S_r$ describes the action of σ on the set of cycles of Γ, ρ_k represents a $(1/n)$ rotation on the k-th cycle, and $0 \le a_k < n$.

Let $0 \le i \le r$. Then an element $\sigma \in \mathcal{G}$ represented as above belongs to $\mathcal{M}_i$ if and only if there exist indices $k_1,\dots,k_i \in \{1,\dots,r\}$ such that π fixes $k_1,\dots,k_i$ and has no other fixed points; and $a_{k_j} > 0$ for $j = 1,\dots,i$. In constructing elements of $\mathcal{M}_i$ we therefore have $d(r,i)$ choices for π, $n-1$ choices for the exponents a_{k_j}, and n choices for the remaining $r-i$ exponents. It follows that $\#\mathcal{M}_i = (n-1)^i \cdot n^{r-i} \cdot d(r,i)$, as required. □

Proof of Theorem 1.5. Let $\Delta(t)$ be the discriminant of Φ_n and let

$$E = \{c \in \mathbb{Q} \mid \Delta(c) = 0\} \cup E_5 \cup E_6 \cup E_7 \cup E_9.$$

By the results of Sections 6 and 7, E is a finite set. Fix $n \in \{5,6,7,9\}$ and $c \in \mathbb{Q} \setminus E$. Since $c \notin E_n$, we have $G_{n,c} \cong G_n$. This implies that $G_{n,c} \equiv G_n$, where $G_{n,c}$ acts on the roots of $\Phi_n(c,x)$. Indeed, since $\Delta(c) \neq 0$, there is a subgroup H of G_n such that $G_{n,c} \equiv H$ (see Theorem 2.9 in [Lang 2002, Chapter VII]). By order considerations, H must be equal to G_n.

Let $S_{n,c}$ be the set of primes p such that $\Phi_n(c,x)$ has a root in $\mathbb{Q}_p$. The fact that $\Delta(c) \neq 0$ implies that $S_{n,c}$ is the complement of $T_{n,c}$. Indeed, every root of $\Phi_n(c,x)$ has period n under ϕ_c; see Theorem 2.4(c) in [Morton and Patel 1994].

Since $G_{n,c} \equiv G_n \equiv \mathcal{G}$, Lemma 8.1 applied to $F(x) = \Phi_n(c,x)$ yields

$$\delta(S_{n,c}) = \frac{\left|\bigcup_{\alpha\in\Gamma} \mathcal{G}_\alpha\right|}{|\mathcal{G}|},$$

where $\mathcal{G}_\alpha$ is the stabilizer of α in $\mathcal{G}$. It follows that $\delta(T_{n,c}) = (\#\mathcal{M})/|\mathcal{G}|$, where $\mathcal{M}$ is defined as in Lemma 8.2. Using this lemma we obtain

$$\begin{aligned}
\delta(T_{5,c}) &= \tfrac{9210721}{6!5^6} \approx 0.8187,\\
\delta(T_{6,c}) &= \tfrac{3095578863701}{9!6^9} \approx 0.8465,\\
\delta(T_{7,c}) &\approx 0.8669,\\
\delta(T_{9,c}) &\approx 0.8948.
\end{aligned}$$

This completes the proof of the theorem. □

9. The exceptional sets E_n

We end this article with a brief discussion concerning the elements of the sets E_n. Recall the following notation introduced in Section 2: S is a splitting field of Φ_n over $\mathbb{Q}(t)$, $G_n = \mathrm{Gal}(S/\mathbb{Q}(t))$, $M_1, \ldots, M_s$ are representatives of the conjugacy classes of maximal subgroups of G_n, and $\mathcal{X}$ is the smooth projective curve with function field S.

Our approach to proving the finiteness of E_n for $n > 4$ is based on Lemma 2.1, which shows that E_n is finite if every quotient curve $\mathcal{X}/M_i$ has genus greater than 1. The proof of the lemma suggests that we may determine the elements of E_n by finding a certain finite set $\mathcal{E}$ and determining all the rational points on the curves $\mathcal{X}/M_i$. The set $\mathcal{E}$ as well as affine models for these curves can be obtained using the methods of the article [Krumm and Sutherland 2017]; however, the rational points on $\mathcal{X}/M_i$ seem impossible to determine due to the large genera of the curves. (For instance, when $n = 5$ one of the curves has genus 9526, as seen in the proof of Theorem 6.6.) Hence, the problem of explicitly determining E_n seems intractable at present. Nevertheless, it is possible to prove some basic results about the elements of E_n.

Proposition 9.1. *For every positive integer n we have $\{0, -2\} \subseteq E_n$.*

Proof. For every $c \in \mathbb{Q}$, the polynomial $\Phi_n(c, x)$ divides $\phi_c^n(x) - x$, where $\phi_c(x) = x^2 + c$. In particular, $\Phi_n(0, x)$ divides $x^{2^n} - x$, which implies that $\Phi_n(0, x)$ splits over a cyclotomic field. It follows that the Galois group $G_{n,0}$ is abelian, hence not isomorphic to G_n, since $G_n \cong (\mathbb{Z}/n\mathbb{Z}) \wr S_r$. Thus $0 \in E_n$.

For $c = -2$ the polynomial ϕ_c is a Chebyshev polynomial satisfying

$$\phi_c(x + 1/x) = x^2 + 1/x^2.$$

We claim that the polynomial $\Phi_n(-2, x)$ splits over the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive $(2^{2n} - 1)$-th root of unity; as above, this will imply that $-2 \in E_n$. Suppose that $\alpha \in \overline{\mathbb{Q}}$ is a root of $\Phi_n(-2, x)$, and let $\beta \in \overline{\mathbb{Q}}$ satisfy $\beta + 1/\beta = \alpha$. Then $\beta^{2^n} + 1/\beta^{2^n} = \beta + 1/\beta$, which implies that $(\beta^{2^n+1} - 1)(\beta^{2^n-1} - 1) = 0$ and hence $\beta^{2^{2n}-1} = 1$. Thus β, and therefore α, belongs to $\mathbb{Q}(\zeta)$. This proves the claim. □

Given a positive integer n for which E_n is finite, one can attempt to find all the elements of E_n by carrying out an exhaustive search within specified height bounds. Recall that the height of a rational

number $\frac{a}{b}$ with $\gcd(a,b)=1$ is given by $\max(|a|,|b|)$. Fixing a height bound h, it a straightforward procedure to construct the set $B(h)$ of all rational numbers having height at most h. One can then construct all the polynomials $\Phi_n(c,x)$ for $c \in B(h)$, compute their Galois groups $G_{n,c}$ (for instance, using the algorithm of Fieker and Klüners [2014], which is implemented in MAGMA), and check whether $G_{n,c} \cong (\mathbb{Z}/n\mathbb{Z}) \wr S_r$. The cost of carrying out this computation grows quickly with n, given the large degree of Φ_n. For $n=7$ the degree of Φ_n is 126, and the above computation is very slow even for small height bounds h. However, for $n=5$ and 6 we have the following result.

Proposition 9.2. *Let $B(h)$ denote the set of all rational numbers with height at most h. Then*

$$E_5 \cap B(50) = \left\{-2, -\tfrac{16}{9}, -\tfrac{3}{2}, -\tfrac{4}{3}, -\tfrac{5}{8}, 0\right\} \quad \textit{and} \quad E_6 \cap B(20) = \{-4, -2, 0\}.$$

References

[Artin 2006] E. Artin, *Algebraic numbers and algebraic functions*, AMS Chelsea Publishing, Providence, RI, 2006. MR Zbl

[Beckmann 1994] S. Beckmann, "On finding elements in inertia groups by reduction modulo p", *J. Algebra* **164**:2 (1994), 415–429. MR Zbl

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Bousch 1992] T. Bousch, *Sur quelques problèmes de dynamique holomorphe*, Ph.D. thesis, Université de Paris-Sud, Centre d'Orsay, 1992.

[Cannon and Holt 2004] J. Cannon and D. F. Holt, "Computing maximal subgroups of finite groups", *J. Symbolic Comput.* **37**:5 (2004), 589–609. MR Zbl

[Dixon and Mortimer 1996] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**, Springer, 1996. MR Zbl

[Dummit and Foote 2004] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Hoboken, NJ, 2004. MR Zbl

[Efrat 2006] I. Efrat, *Valuations, orderings, and Milnor K-theory*, Mathematical Surveys and Monographs **124**, Amer. Math. Soc., Providence, RI, 2006. MR Zbl

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR Zbl

[Fieker and Klüners 2014] C. Fieker and J. Klüners, "Computation of Galois groups of rational polynomials", *LMS J. Comput. Math.* **17**:1 (2014), 141–158. MR Zbl

[Flynn et al. 1997] E. V. Flynn, B. Poonen, and E. F. Schaefer, "Cycles of quadratic polynomials and rational points on a genus-2 curve", *Duke Math. J.* **90**:3 (1997), 435–463. MR Zbl

[Frucht 1949] R. Frucht, "On the groups of repeated graphs", *Bull. Amer. Math. Soc.* **55** (1949), 418–420. MR Zbl

[Harary 1969] F. Harary, *Graph theory*, Addison-Wesley Publishing Co., Reading, MA, 1969. MR Zbl

[Kerber 1971] A. Kerber, *Representations of permutation groups, I*, Lecture Notes in Mathematics **240**, Springer, 1971. MR Zbl

[Krumm 2016] D. Krumm, "A local-global principle in the dynamics of quadratic polynomials", *Int. J. Number Theory* **12**:8 (2016), 2265–2297. MR Zbl

[Krumm 2018a] D. Krumm, "code for the computations in the article "A finiteness theorem for specializations of dynatomic polynomials"", 2018, Available at https://github.com/davidkrumm/finiteness_dynatomic. Magma code.

[Krumm 2018b] D. Krumm, "Galois groups in a family of dynatomic polynomials", *J. Number Theory* **187** (2018), 469–511. MR Zbl

[Krumm and Sutherland 2017] D. Krumm and N. Sutherland, "Galois groups over rational function fields and explicit Hilbert irreducibility", preprint, 2017. arXiv

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, 2002. MR Zbl

[Leon 1997] J. S. Leon, "Partitions, refinements, and permutation group computation", pp. 123–158 in *Groups and computation, II* (New Brunswick, NJ, 1995), edited by L. Finkelstein and W. M. Kantor, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **28**, Amer. Math. Soc., Providence, RI, 1997. MR Zbl

[Morton 1992] P. Morton, "Arithmetic properties of periodic points of quadratic maps", *Acta Arith.* **62**:4 (1992), 343–372. MR Zbl

[Morton 1996] P. Morton, "On certain algebraic curves related to polynomial maps", *Compositio Math.* **103**:3 (1996), 319–350. MR Zbl

[Morton 1998] P. Morton, "Arithmetic properties of periodic points of quadratic maps, II", *Acta Arith.* **87**:2 (1998), 89–102. MR Zbl

[Morton and Patel 1994] P. Morton and P. Patel, "The Galois theory of periodic points of polynomial maps", *Proc. London Math. Soc.* (3) **68**:2 (1994), 225–263. MR Zbl

[Morton and Vivaldi 1995] P. Morton and F. Vivaldi, "Bifurcations and discriminants for polynomial maps", *Nonlinearity* **8**:4 (1995), 571–584. MR Zbl

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **322**, Springer, 1999. MR Zbl

[Poonen 1998] B. Poonen, "The classification of rational preperiodic points of quadratic polynomials over $\mathbf{Q}$: a refined conjecture", *Math. Z.* **228**:1 (1998), 11–29. MR Zbl

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer, 2002. MR Zbl

[Rotman 1995] J. J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics **148**, Springer, 1995. MR Zbl

[Serre 2008] J.-P. Serre, *Topics in Galois theory*, 2nd ed., Research Notes in Mathematics **1**, A K Peters, Ltd., Wellesley, MA, 2008. MR

[Stanley 2012] R. P. Stanley, *Enumerative combinatorics, Volume 1*, 2nd ed., Cambridge Studies in Advanced Mathematics **49**, Cambridge University Press, 2012. MR Zbl

[Stichtenoth 2009] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics **254**, Springer, 2009. MR Zbl

[Stoll 2008] M. Stoll, "Rational 6-cycles under iteration of quadratic polynomials", *LMS J. Comput. Math.* **11** (2008), 367–380. MR Zbl

Communicated by Joseph H. Silverman
Received 2018-05-28 Revised 2019-01-22 Accepted 2019-02-22

dkrumm@reed.edu *Reed College, Portland, OR, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US $385/year for the electronic version, and $590/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 13 No. 4 2019