8-30-2021 3:00 PM

Genus Bounds for Some Dynatomic Modular Curves

Andrew W. Herring, *The University of Western Ontario*

Supervisor: Hall, Chris J., *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Mathematics

Abstract

We prove that for every $n \geq 10$ there are at most finitely many values $c \in \mathbb{Q}$ such that the quadratic polynomial $x^2 + c$ has a point $\alpha \in \mathbb{Q}$ of period n. We achieve this by proving that for these values of n, every n-th dynatomic modular curve has genus at least two.

Keywords: Arithmetic dynamics, modular curves, genus

Summary for Lay Audience

Number theory studies properties of integers $(\ldots, -2, -1, 0, 1, 2, \ldots)$ and rational numbers (numbers which are "fractions"). While it is easy to come up with "good enough" approximations to solutions to polynomial equations using a computer, it can be much (and sometimes much, much) harder to find exact solutions which are integers or rational numbers.

A dynamical system is some function f whose outputs and inputs come from the same set S. Whenever this is the case, we can "iterate" f. By this we mean that we can start from some input $a \in S$ and apply f to a to get output $f(a)$, and then apply f to $f(a)$ to get output $f(f(a))$, and then apply f to $f(f(a))$ to get $f(f(f(a)))$ and so on. For many, things start to get interesting when you perform some number of iterations and get back the original input a you started with. When this happens a is called a periodic point for f, and the smallest number of iterations which gets you back to a is called the period.

In arithmetic dynamics, we look at dynamical systems from the point of view of number theory. The present thesis is concerned with showing that for the polynomial dynamical system $f_c(x) = x^2 + c$ where c is some rational number, periodic points which are rational numbers are extremely rare. A big conjecture in arithmetic dynamics states that there are no periodic points of period 4 or larger for $f_c(x)$. In some sense, this thesis shows that the number of possible exceptions to the big conjecture is finite. Previously, this was only known for points of period 5, 6, 7, and 9. Here we show that this also holds for any period at least 10.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This research belongs to the relatively young mathematical discipline of arithmetic dynamics in which we study dynamical systems from the point of view of number theory. An excellent survey of some of the open problems in arithmetic dynamics is given in [1].

1.1 Polynomial dynamical systems

Let F be any perfect field, and $\bar{F}$ a fixed algebraic closure. Each non-constant polynomial $g(x) \in F[x]$ determines a **polynomial dynamical system**, by which we mean a map $g : \bar{F} \to \bar{F}$ sending α to $g(\alpha)$. For each non-negative integer k, the **k-fold composition** of g is the polynomial

$$g^k(x) := \begin{cases} x, & \text{for } k = 0; \\ g(x), & \text{for } k = 1; \\ g(g^{k-1}(x)), & \text{for } k \geq 2. \end{cases}$$

An element $\alpha \in \bar{F}$ is **periodic for** g (or **g-periodic**) if there is some positive integer k for which $g^k(\alpha) = \alpha$.

For any polynomial $h(x) \in \bar{F}[x]$, the **(geometric) zero set of** h is the set

$$Z(h) := \{\beta \in \bar{F} : h(\beta) = 0\}.$$

Thus $\alpha \in \bar{F}$ is g-periodic if and only if

$$\alpha \in \mathrm{Per}(g) := \bigcup_{k \geq 1} Z\left(g^k(x) - x\right).$$

For each $\alpha \in \mathrm{Per}(g)$, there is a well-defined positive integer n for which $g^n(\alpha) = \alpha$, but $g^k(\alpha) \neq \alpha$ for every $k < n$. We say that α has **period** n for g, or equivalently, that α is **n-periodic** for g.

For any subset $S \subset \bar{F}$, define

$$\mathrm{Per}_n(g; S) := \{\alpha \in S : \alpha \text{ is } n\text{-periodic for } g\}$$

to be the **set of all n-periodic points for g in S**. (When $S = \bar{F}$, we simplify notation: $\mathrm{Per}_n(g) := \mathrm{Per}_n(g; \bar{F})$).

Example 1.1.1. In this example we will describe the sets $\mathrm{Per}_1(x^2-1;\mathbb{Q})$ and $\mathrm{Per}_2(x^2-1;\mathbb{Q})$. Let $h(x) := x^2 - 1 \in \mathbb{Q}[x]$.

A rational number $\alpha \in \mathbb{Q}$ is 1-periodic for h (or equivalently, α is a **fixed point** of h) if and only if $\alpha \in Z(h(x)-x) \cap \mathbb{Q} = Z(x^2-x-1) \cap \mathbb{Q}$. But the discriminant of x^2-x-1 is 5 which is not a square in $\mathbb{Q}$. Therefore x^2-x-1 has no roots in $\mathbb{Q}$ and $\mathrm{Per}_1(x^2-1;\mathbb{Q}) = \emptyset$.

If $\alpha \in \mathrm{Per}_2(h(x);\mathbb{Q})$, then $\alpha \in Z(h^2(x)-x) \cap \mathbb{Q}$.We have

$$h^2(x) - x = (x^2-1)^2 - 1 - x = x^4 - 2x^2 - x = x(x^3 - 2x - 1),$$

and we have found that $h^2(0) - 0 = 0$. In fact this shows that $0 \in \mathrm{Per}_2(h(x);\mathbb{Q})$, since $h(0) \neq 0$. At this point we apply an easy but important result: for any polynomial dynamical system g we have $g^m(x) - x \mid g^{km}(x) - x$ for all positive integers m, k. In particular, $h(x) - x \mid h^2(x) - x$:

$$h^2(x) - x = x^4 - 2x^2 - x = (x^2 - x - 1)(x^2 + x) = x(x+1)(x^2 - x - 1)$$

Thus $Z(h^2(x)-x) \cap \mathbb{Q} = \{0, -1\}$, and in fact $\mathrm{Per}_2(h(x);\mathbb{Q}) = \{0,-1\}$ since $h^2(0) = 0$ but $h(0) = -1 \neq 0$ and $h^2(-1) = -1$, but $h(-1) = 0 \neq -1$.

1.2 Motivating problem

For $c \in \mathbb{Q}$, consider the quadratic polynomial $f_c(x) := x^2 + c \in \mathbb{Q}[x]$. Up to a linear change of variables, every quadratic polynomial in $\mathbb{Q}[x]$ has the form $f_c(x)$ for some $c \in \mathbb{Q}$. This thesis studies the possible periodic points in $\mathbb{Q}$ of these $f_c(x)$ motivated by the following conjecture due to Flynn, Poonen, and Schaefer:

Conjecture 1.2.1 ([5]). *Let $c \in \mathbb{Q}$. If $\mathrm{Per}_n(f_c;\mathbb{Q})$ is non-empty, then $n \in \{1,2,3\}$.*

Conjecture 1.2.1 is solved in the cases $n = 4$, $n = 5$, and $n = 6$ by [11], [5], and [17] respectively, although the proof in the $n = 6$ case is conditional on the Birch and Swinnerton-Dyer conjecture.

It is also known ([8]) that for $n \in \{5,6,7,9\}$ there are at most finitely many $c \in \mathbb{Q}$ such that $f_c(x)$ has a point of period n in $\mathbb{Q}$; in this thesis, we prove that the same is true for every $n \geq 10$ (Theorem 7.0.1).

1.3 Dynatomic polynomials and their Galois groups

Let t be transcendental over $\mathbb{C}$. We consider $K_0 := \mathbb{Q}(t)$, the **rational function field over** $\mathbb{Q}$, and sitting inside K_0 the polynomial ring $A_0 := \mathbb{Q}[t]$. The polynomial $f(x) := x^2 + t \in A_0[x]$ is called the **(generic) quadratic polynomial** over $\mathbb{Q}$. Notice that every $f_c(x)$ is a specialization of $f(x)$:

$$f_c(x) = x^2 + c = (x^2 + t) \mid_{t=c} = f(x) \mid_{t=c} .$$

Our strategy then is to study the dynamics of $f_c(x)$ for each $c \in \mathbb{Q}$ by studying the dynamics of $f(x)$. Fix a positive integer n.

Definition 1.3.1. The **(generic) n-th dynatomic polynomial** (of $f(x)$) is

$$\Phi_n(x) := \prod_{d|n} \left(f^d(x) - x\right)^{\mu(n/d)},$$

where $\mu : \mathbb{Z}_{>0} \to \{0, \pm 1\}$ is the **Mobius function** given by $\mu(1) := 1$ and

$$\mu\left(p_1^{e_1} \dots p_r^{e_r}\right) := \begin{cases} 0, & \text{if } e_j \geq 2 \text{ for some } j \in [r]; \\ (-1)^r, & \text{else.} \end{cases}$$

We let $Z := Z(\Phi_n(x))$ denote the **(geometric) zero set of** $\Phi_n(x)$.

Example 1.3.2. We have

$$\begin{aligned} \Phi_1(x) &= x^2 - x + t \\ \Phi_2(x) &= x^2 + x + t + 1 \\ \Phi_3(x) &= x^6 + x^5 + (3t+1)x^4 + (2t+1)x^3 + \left(3t^2 + 3t + 1\right)x^2 \\ &\quad + \left(t^2 + 2t + 1\right)x + t^3 + 2t^2 + t + 1 \end{aligned}$$

The next result gives that $\Phi_n(x)$ is an absolutely irreducible polynomial whose zeros are precisely the n-periodic points of $f(x)$.

Proposition 1.3.3. *The following hold:*

(1) $\Phi_n(x) \in A_0[x]$*;*

(2) $\Phi_n(x)$ *is irreducible over* $\mathbb{C}(t)$*;*

(3) $Z = \mathrm{Per}_n(f)$*;*

(4) $\Phi_n(x) \mid \Phi_n(f(x))$.

Proof. See [12] for (1) and (4), and see [2] for (2). Statement (3) follows from (2). □

It follows from (4) of Proposition 1.3.3 that for every $\alpha \in Z$, we have $\{f^j(\alpha) : j \geq 0\} \subseteq Z$. Indeed, (4) implies that $Z \subseteq Z(\Phi_n(f(x)))$. Thus if $\alpha \in Z$, then $\Phi_n(f(\alpha)) = 0$ which shows $f(\alpha) \in Z$, and so by induction $f^j(\alpha) \in Z$ for every positive integer j.

But now by (3) of Proposition 1.3.3, $\alpha \in Z = \mathrm{Per}_n(f)$ implies that $f^n(\alpha) = \alpha$ and $f^k(\alpha) \neq \alpha$ for every $k < n$. Thus $\{f^j(a) : j \geq 0\} = \{\alpha, f(\alpha), f^2(\alpha), \dots, f^{n-1}(\alpha)\}$, and this second set has precisely n elements. Notice that this implies that $n \mid \deg \Phi_n(x)$ since a single root $\alpha \in Z$ gives rise to n distinct roots $\alpha, f(\alpha), \dots, f^{n-1}(\alpha) \in Z$. We have proved the following:

Corollary 1.3.4. *If we let* r *denote the positive integer* $r = \frac{\deg \Phi_n(x)}{n}$*, then we can partition* Z *as*

$$Z = \bigsqcup_{i=1}^{r} A_i$$

where $A_i = \{\alpha_i, f(\alpha_i), \dots, f^{n-1}(\alpha_i)\}$ *for some* $\alpha_i \in L_0$ *for every* $i = 1, \dots, r$.

For each $i \in [r]$, the set A_i is called an **f-orbit**.

Let L_0 denote the **splitting field of $\Phi_n(x)$ over K_0**.The extension L_0/K_0 is Galois and we define $G := \mathrm{Gal}(L_0/K_0)$ to be the Galois group, which we will call the **(generic) n-th dynatomic Galois group**.

For $c \in \mathbb{Q}$,

$$\Phi_{n,c}(x) := \prod_{d|n} \left(f_c^d(x) - x\right)^{\mu(n/d)} \in \mathbb{Q}[x]$$

is the **n-th dynatomic polynomial (specialized) at c**. Then $\Phi_{n,c}(x) = \Phi_n(x) \mid_{t=c}$ so that $\Phi_{n,c}(x)$ is the specialization of $\Phi_n(x)$ at $t = c$. Let $Z_c := Z(\Phi_{n,c}(x))$ denote the **(geometric) zero set of $\Phi_{n,c}(x)$**.

We have $\mathrm{Per}_n(f_c) \subset Z_c$, but unlike in the generic case, the reverse containment does not hold in general. It is also the case that there exist values $c \in \mathbb{Q}$ for which $\Phi_{n,c}(x)$ is reducible over $\mathbb{Q}$.

We define $L_{0,c}$ to be the **splitting field of $\Phi_{n,c}(x)$ over $\mathbb{Q}$**. Then $L_{0,c}/\mathbb{Q}$ is Galois and we define $G_c := \mathrm{Gal}(L_{0,c}/\mathbb{Q})$ to be the Galois group, called the **n-th dynatomic Galois group (specialized) at c**.

1.4 Exceptional values and periodic points in $\mathbb{Q}$

Define

$$D_n := \{c \in \mathbb{Q} : \ \Phi_{n,c}(x) \text{ is inseparable}\}.$$

As we will see in Corollary 2.3.7, if $c \in \mathbb{Q} - D_n$, then G_c is a subgroup of G. Since D_n is a finite set, we have $G_c \leq G$ for all but finitely many $c \in \mathbb{Q}$.

Definition 1.4.1. For each positive integer n, we define a set

$$E_n := \{c \in \mathbb{Q} - D_n : G_c \lneq G\}$$

and call it the **n-th exceptional set**. Values $c \in E_n$ are called **exceptional values**.

Exceptional values are related to n-periodic points via the following result (Theorem 2.3.8): if $c \in \mathbb{Q} - D_n$ and $\mathrm{Per}_n(f_c; \mathbb{Q})$ is non-empty (so that f_c has some n-periodic point in $\mathbb{Q}$), then $c \in E_n$. Thus, in order to prove that for a given n there are only finitely many values $c \in \mathbb{Q}$ for which f_c has a point of period n in $\mathbb{Q}$, it suffices to show that E_n is finite. (We remark that according to Hilbert's Irreducibility Theorem ([15, Proposition 3.3.5]), the set E_n is known to be "thin." Thin sets are small (in a suitably defined sense), but there are still thin sets which are infinite.)

1.5 Rational points on modular curves and genus

Saying that $c \in E_n$ is the same as saying that c lies beneath a $\mathbb{Q}$-rational point on some "dynatomic modular curve" (Theorem 3.2.5). Therefore, to show that E_n is finite, it is enough to show that the set of $\mathbb{Q}$-rational points of each such dynatomic modular curve is finite. By Faltings' Theorem 3.2.2, if a curve defined over $\mathbb{Q}$ has genus at least 2 then it has at most finitely

many $\mathbb{Q}$-rational points. We use ramification theory together with the Riemann-Hurwitz genus formula 3.2.4 to produce lower bounds on genus, and then apply Faltings' Theorem.

A key reduction along the way is noting that it suffices to consider dynatomic modular curves X_M for *maximal* subgroups of G. Such maximal subgroups M come in two distinct flavors which we call "chocolate" (Lemma 6.1.1) and "vanilla" (Lemma 6.1.2). Vanilla maximal subgroups are identified with subgroups of $(\mathbb{Z}/n)^r$ which are invariant under the action of S_r which permutes the factors $\mathbb{Z}/n$. In particular, the fact that $(\mathbb{Z}/n)^r$ is abelian allows us to use very nice techniques from the theory of S_r-modules. Chocolate maximal subgroups are significantly more complicated in that they are identified with maximal subgroups of the non-abelian (for $r \geq 3$) group S_r. Fortunately, a Theorem of Guralnick and Shareshian does much of the heavy lifting in this case; see Theorem 6.3.2.

1.6 Overview of the thesis

In Chapter 2, we lay a foundation in algebraic number theory. We study extensions of Dedekind domains, prime factorization, the action of a Galois group on prime ideals, and decomposition and inertia groups. We then see how to compute ramification indices in intermediate field extensions in terms of group theoretic data. Finally, we apply the theory of decomposition and inertia groups to show that the specialized dynatomic Galois group is almost always a subgroup of its generic counterpart.

In Chapter 3, we study curves, function fields, and genus. We begin by reviewing an important categorical equivalence which says that function fields over $\mathbb{Q}$ and curves defined over $\mathbb{Q}$ are one in the same. Next we discuss the genus of a curve, and the arithmetic consequences which can be deduced from genus. We will see that genus can be computed "geometrically," and then we present our main tool for bounding genus: the Riemann-Hurwitz genus formula. At the end of the chapter, we apply all this "abstract non-sense" to our main problem by connecting rational points on dynatomic modular curves and exceptional values.

A central player in this thesis is the dynatomic Galois group G; knowing the structure of G is integral to our program. In Chapter 4, we review semi-direct products in general, and then work hard to convince ourselves that G has the structure of a particular semi-direct product. Much of the material in this chapter was proved by Bousch ([2]), although we found it necessary to reformulate several arguments in our preferred language and notation.

In Chapter 5, we consider the ramification theory of dynatomic polynomials. While much was already known, we invested significant energy to precisely identify all but a few inertia subgroups of G in terms of the semi-direct product description of G from Chapter 4.

Chapter 6 is where we finally get our hands dirty with genus bounds for dynatomic modular curves. There is a helpful dichotomy for maximal subgroups of G which partitions the maximal subgroups into two flavors: "chocolate" and "vanilla." For vanilla maximal subgroups, we can use the theory of Γ-modules together with basic Sylow theory to precisely compute many ramification indices. Chocolate maximal subgroups (as we hope the name suggests) are more complicated. Fortunately Guralnick and Shareshian have genus bounds which enable us to handle the chocolate maximals.

Chapter 7 is a victory lap. It contains only a single theorem which ties together several results from elsewhere into our main result: that for every $n \geq 10$, there are at most finitely

many rational numbers $c \in \mathbb{Q}$ such that $x^2 + c$ has a point of period n in $\mathbb{Q}$.

Chapter 2

Galois theory and ramification theory

2.1 Group actions

Let G be any finite group, and Ω any finite set. A **(left) group action** of G on Ω is a function

$$\begin{aligned} G \times \Omega &\longrightarrow \Omega \\ (g, x) &\longmapsto {}^{g}x \end{aligned}$$

satisfying the following conditions:

1. ${}^{1}x = x$ for every $x \in \Omega$;
2. for all $g_1, g_2 \in G$ and every $x \in \Omega$ we have

$$ {}^{(g_2 g_1)}x = {}^{g_2}\left({}^{g_1}x\right). $$

In this situation, we say that G **acts on** Ω and that Ω is a **(left)** G**-set**. If $|\Omega| = n$, then we say that G is a **permutation group of degree** n.

Our preference throughout this work will be to work with *left* group actions, so we will frequently drop the modifier "(left)" and speak of group actions and G-sets. If it becomes necessary to consider groups acting on the *right*, we will make it explicit when speaking of right group actions.

Suppose Ω is a G-set. Then there is an induced homomorphism

$$\begin{aligned} \rho : \ G &\longrightarrow \mathrm{Sym}\,(\Omega) \\ g &\longmapsto \rho_g, \end{aligned}$$

where $\rho_g(x) := {}^{g}x$ for each $x \in \Omega$. The homomorphism ρ is called the **permutation representation** of the action of G on Ω. If $\ker(\rho) = \{1\}$, then we say that G acts **faithfully** on Ω.

Suppose now that Ω_1 and Ω_2 are two G-sets. A function $\phi : \Omega_1 \to \Omega_2$ is G**-equivariant** if for every $x \in \Omega_1$ and every $g \in G$ we have that

$$\phi\left({}^{g}x\right) = {}^{g}\phi(x).$$

The collection of all G-sets forms a category G-**Set**, where morphisms are G-equivariant maps. (Thus, an isomorphism of G-sets is any G-equivariant bijection).

Let G be a finite group and $\Omega \in G$-**Set**. For $x \in \Omega$, the **orbit** containing x is

$$G \cdot x := \{{}^g x : g \in G\}.$$

The collection of all orbits forms a partition on Ω. If there is only one orbit, then we say that G acts **transitively** on Ω, or that Ω is a **transitive** G-**set**. Equivalently, G acts transitively on Ω if for all $x, y \in \Omega$, there is some $g \in G$ with ${}^g x = y$.

An extremely useful example of a transitive group action comes from Galois theory. If E/F is a Galois extension of fields, then $\mathrm{Gal}(E/F)$ acts transitively on the zeros of any $h(x) \in F[x]$ which is F-irreducible and which has some root (hence all of its roots) in E.

For $x \in \Omega$, the **stabilizer of** x **in** G is

$$G_x := \{g \in G : {}^g x = x\}.$$

For every $x \in \Omega$, the stabilizer G_x is a subgroup of G.

Lemma 2.1.1. *Let $\Omega \in G$-**Set**. The following hold:*

1. *For each $x \in \Omega$ there is an isomorphism of G-sets*

$$\begin{aligned} G \cdot x &\longrightarrow G/G_x \\ {}^g x &\longmapsto gG_x, \end{aligned}$$

   where the action of G on the coset space G/G_x is given by ${}^h(gG_x) = (hg)G_x$. In particular, we have that $|G \cdot x| = [G : G_x]$.

2. *For each $x \in \Omega$ we have*

$$G_{{}^g x} = {}^g G_x,$$

   where ${}^g G_x := gG_x g^{-1}$ is the image of G_x under g-conjugation.

Now suppose we have groups G and H together with sets $X \in G$-**Set** and $Y \in H$-**Set**. Then these actions are **isomorphic group actions** provided that there is a group isomorphism $\phi : G \to H$ together with a bijection $f : X \to Y$ such that

$$f({}^g x) = {}^{\phi(g)} \sigma(x)$$

for every $g \in G$ and every $x \in X$.

2.2 Galois action on primes

2.2.1 Dedekind extensions and prime factorization

Following the lead of [19], we will adopt a shorthand for a frequent set of hypotheses. By "assume $AKLB$" we mean "assume that A is a Dedekind domain, K is the fraction field of A, L is a finite separable field extension of K, and B is the integral closure of A in L."

So assume $AKLB$. It is a fact that under the $AKLB$ assumptions, B is a Dedekind domain with fraction field L, and that $B \cap K = A$. Let R be any Dedekind domain with fraction field F. By a **prime of** R (or equivalently, **a prime of** F), we mean any non-zero prime ideal of R. We will abuse notation and write $\mathrm{spec}\,(R)$ (or even $\mathrm{spec}\,(F)$) for the **set of all primes of** R. Thus, since $A \subseteq B$ is an extension of Dedekind domains, for every $\mathfrak{p} \in \mathrm{spec}\,(A)$, there exist $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in \mathrm{spec}\,(B)$ together with positive integers $e_1, \ldots, e_r$ such that

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_r^{e_r} \tag{2.1}$$

and this factorization is unique up to a reordering of the $\mathfrak{q}_i^{e_i}$. Each prime $\mathfrak{q}_i$ appearing in 2.1 is said to **lie over/lie above** $\mathfrak{p}$, and we indicate this relationship by writing $\mathfrak{q}_i \mid \mathfrak{p}$. It is a fact that $\mathfrak{q} \mid \mathfrak{p}$ if and only if $\mathfrak{q} \cap A = \mathfrak{p}$. We define $\mathbb{P}_L(\mathfrak{p}) := \{\text{primes } \mathfrak{q} \text{ of } L : \mathfrak{q} \mid \mathfrak{p}\}$ to be the **set of all primes of** L **lying over** $\mathfrak{p}$.

Let R be any Dedekind domain and $\mathfrak{p} \in \mathrm{spec}\,(R)$. Since $\mathfrak{p}$ is a non-zero prime and R has dimension 1, in fact $\mathfrak{p}$ is a *maximal* ideal of R, and thus the quotient $R/\mathfrak{p}$ is a field called the **residue field**, which we will denote by $\kappa(\mathfrak{p})$. Thus, under the $AKLB$ framework, we have residue fields $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ and $\kappa(\mathfrak{q}) = B/\mathfrak{q}$ for all primes $\mathfrak{p}$ of A and $\mathfrak{q}$ of B. If $\mathfrak{p}$ is a prime of A and $\mathfrak{q} \mid \mathfrak{p}$, then $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is a field extension of finite degree which we call the **residue field extension of** $\mathfrak{q} \mid \mathfrak{p}$.

Definition 2.2.1. Assume $AKLB$, fix a prime $\mathfrak{p}$ of A, and suppose that

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_r^{e_r}$$

is the unique factorization of $\mathfrak{p}B$ into primes of B. The exponent e_i, which we will interchangeably denote by $e_i \equiv e(\mathfrak{q}_i \mid \mathfrak{p}) \equiv e_{\mathfrak{q}_i}$ depending on the context, is the **ramification index** of $\mathfrak{q}_i \mid \mathfrak{p}$.

The degree

$$f_i \equiv f(\mathfrak{q}_i \mid \mathfrak{p}) \equiv f_{\mathfrak{q}_i} := [\kappa(\mathfrak{q}_i) : \kappa(\mathfrak{p})]$$

is the **residue degree** of $\mathfrak{q}_i \mid \mathfrak{p}$.

We say that $\mathfrak{q}_i \mid \mathfrak{p}$ is **unramified** if $e(\mathfrak{q}_i \mid \mathfrak{p}) = 1$ and the residue field extension $\kappa(\mathfrak{q}_i)/\kappa(\mathfrak{p})$ is separable; otherwise $\mathfrak{q}_i \mid \mathfrak{p}$ is **ramified**. Finally, $\mathfrak{p}$ is **unramified in** B provided that $\mathfrak{q}_i \mid \mathfrak{p}$ is unramified for every $\mathfrak{q}_i \in \mathbb{P}_L(\mathfrak{p})$.

Proposition 2.2.2. *Assume $AKLB$. The following hold:*

1. *For every prime $\mathfrak{p}$ of A, we have*

$$\sum_{\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})} e(\mathfrak{q} \mid \mathfrak{p}) f(\mathfrak{q} \mid \mathfrak{p}) = [L : K]. \tag{2.2}$$

2. *Assume further that M/L is another finite separable extension, and that C is the integral closure of A in M. Then C is the integral closure of B in M. Let $\mathfrak{p}$ be a prime of A and consider $\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})$ and $\mathfrak{r} \in \mathbb{P}_M(\mathfrak{q})$. Then $\mathfrak{r} \in \mathbb{P}_M(\mathfrak{p})$ and we have that*

$$e(\mathfrak{r} \mid \mathfrak{p}) = e(\mathfrak{r} \mid \mathfrak{q}) e(\mathfrak{q} \mid \mathfrak{p}), \text{ and } f(\mathfrak{r} \mid \mathfrak{p}) = f(\mathfrak{r} \mid \mathfrak{q}) f(\mathfrak{q} \mid \mathfrak{p}).$$

The next result due to Dedekind and Kummer gives a practical method for determining how a prime ramifies.

Theorem 2.2.3 ([19, Theorem 6.14])**.** *Let R be a Dedekind domain with fraction field F, let E be a finite separable extension of F, and let S denote the integral closure of R in E. (In other words, assume that $RFES$ satisfies the conditions of $AKLB$). Assume that $E = F(\beta)$, and $\beta \in S$. Let $m(x) \in R[x]$ be the minimal polynomial of β, let P be any prime of R, and let*

$$\overline{m}(x) = \overline{g_1}(x)^{e_1} \dots \overline{g_s}(x)^{e_s}$$

be its factorization into monic irreducibles $\overline{g_i}(x)$ of $(R/P)[x]$. Define $Q_i := (P, g_i(\beta))$, where $g_i(x) \in R[x]$ is any lift of $\overline{g_i}(x) \in (R/P)[x]$ to $R[x]$. If $S = R[\beta]$, then

$$PS = Q_1^{e_1} \dots Q_s^{e_s}$$

is the factorization of PS in S, and the reside degree of Q_i is $\deg \overline{g_i}(x)$.

2.2.2 Decomposition and inertia subgroups

By "assume $AKLBG$" we mean "assume $AKLB$, and further assume that L/K is a Galois extension with $G := \mathrm{Gal}(L/K)$." For the remainder of the subsection, assume $AKLBG$ and fix a prime $\mathfrak{p}$ of A.

Proposition 2.2.4. *The following hold:*

1. *We have a transitive action of G on $\mathbb{P}_L(\mathfrak{p})$ defined by*

$$^g\mathfrak{p} := g(\mathfrak{p}) = \{g(a) : a \in \mathfrak{p}\}.$$

2. *For all $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathbb{P}_L(\mathfrak{p})$ we have*

$$e(\mathfrak{q}_1 \mid \mathfrak{p}) = e(\mathfrak{q}_2 \mid \mathfrak{p}), \text{ and } f(\mathfrak{q}_1 \mid \mathfrak{p}) = f(\mathfrak{q}_2 \mid \mathfrak{p}).$$

Under the $AKLBG$ setup, Proposition 2.2.4 shows that the ramification indices $e(\mathfrak{q} \mid \mathfrak{p})$ and residue degrees $f(\mathfrak{q} \mid \mathfrak{p})$ are independent of the choice of $\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})$, so in this situation we will sometimes simplify notation and write $e_\mathfrak{p}$ and $f_\mathfrak{p}$ for $e(\mathfrak{q} \mid \mathfrak{p})$ and $f(\mathfrak{q} \mid \mathfrak{p})$ respectively. As an immediate corollary to Propositions 2.2.4 and 2.2.2, we have that

$$[L : K] = \sum_{\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})} e(\mathfrak{q} \mid \mathfrak{p}) f(\mathfrak{q} \mid \mathfrak{p}) = |\mathbb{P}_L(\mathfrak{p})|\, e_\mathfrak{p} f_\mathfrak{p}. \tag{2.3}$$

Definition 2.2.5. Let $\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})$. The **decomposition group of** $\mathfrak{q} \mid \mathfrak{p}$, denoted by $D(\mathfrak{q} \mid \mathfrak{p})$ or equivalently by $D_\mathfrak{q}$, is defined to be the stabilizer $G_\mathfrak{q}$ of $\mathfrak{q}$ under the (transitive) action of G on $\mathbb{P}_L(\mathfrak{p})$.

Lemma 2.2.6. *We have the following:*

1. *$D({}^{g}\mathfrak{q} \mid \mathfrak{p}) = {}^{g}D(\mathfrak{q} \mid \mathfrak{p})$ for every $\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})$ and every $g \in G$. Consequently any two decomposition groups $D(\mathfrak{q}_1 \mid \mathfrak{p})$ and $D(\mathfrak{q}_2 \mid \mathfrak{p})$ are conjugates in G, and in particular are isomorphic.*

2. *For every $\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})$, we have $|D(\mathfrak{q} \mid \mathfrak{p})| = e_{\mathfrak{p}} f_{\mathfrak{p}}$.*

Proof. 1. The first statement is 2 of Lemma 2.1.1 applied to the particular stabilizer $D(\mathfrak{q} \mid \mathfrak{p})$, and the second follows from the first together with transitivity of the Galois action: for any $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathbb{P}_L(\mathfrak{p})$ there is some $g \in G$ with ${}^{g}\mathfrak{q}_1 = \mathfrak{q}_2$.

2. By 1 of Lemma 2.1.1 and transitivity, we have

$$|\mathbb{P}_L(\mathfrak{p})| = |G \cdot \mathfrak{q}| = \frac{|G|}{|D(\mathfrak{q} \mid \mathfrak{p})|}.$$

But now, $|G| = [L : K] = |\mathbb{P}_L(\mathfrak{p})| e_{\mathfrak{p}} f_{\mathfrak{p}}$ by 2.3, so we get the desired result by rearranging and substituting.

□

Fix $\mathfrak{q} \in \mathbb{P}_L(\mathfrak{p})$. For every $\sigma \in G$, it is a straight forward application of the definitions which shows that $\sigma(B) = B$. Therefore, $\sigma|_B$ is a ring automorphism of B which restricts to Id_A on A: in particular, $\sigma(a) = a$ for every $a \in \mathfrak{p}$. Consider the induced map $\bar{\sigma} : \kappa(\mathfrak{q}) \to \kappa(\sigma(\mathfrak{q}))$ given by

$$\bar{\sigma}(\bar{b}) \equiv \bar{\sigma}(b \pmod{\mathfrak{q}}) := \overline{\sigma(b)} \equiv \sigma(b) \pmod{\sigma(\mathfrak{q})}.$$

Both $\kappa(\mathfrak{q})$ and $\kappa(\sigma(\mathfrak{q}))$ are residue field extensions of $\kappa(\mathfrak{p})$, and the discussion above shows that $\bar{\sigma}|_{\kappa(\mathfrak{p})} = \mathrm{Id}_{\kappa(\mathfrak{p})}$. Therefore, $\bar{\sigma} \in \mathrm{Hom}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q}), \kappa(\sigma(\mathfrak{q})))$ is an isomorphism of $\kappa(\mathfrak{p})$-extensions.

Now, if we take $\sigma \in D(\mathfrak{q} \mid \mathfrak{p})$, then $\sigma(\mathfrak{q}) = \mathfrak{q}$, and $\bar{\sigma}$ is an automorphism of the residue extension $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$: that is,

$$\bar{\sigma} \in \mathrm{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q})).$$

Proposition 2.2.7. *The map*

$$\begin{aligned} \pi_{\mathfrak{q}} : \ D(\mathfrak{q} \mid \mathfrak{p}) &\longrightarrow \mathrm{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q})) \\ \sigma &\longmapsto \bar{\sigma} \end{aligned}$$

is a surjective group homomorphism, and the residue field extension $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is normal.

Definition 2.2.8. The kernel of $\pi_{\mathfrak{q}}$ is the **inertia group** of $\mathfrak{q} \mid \mathfrak{p}$, and is denoted by $I(\mathfrak{q} \mid \mathfrak{p})$ or by $I_{\mathfrak{q}}$.

In other words,

$$I(\mathfrak{q} \mid \mathfrak{p}) = \{\sigma \in G : \sigma(b) \equiv b \pmod{\mathfrak{q}}, \text{ for all } b \in B\}.$$

Corollary 2.2.9. *The following hold:*

1. *There is a short exact sequence*

$$1 \longrightarrow I(\mathfrak{q} \mid \mathfrak{p}) \longrightarrow D(\mathfrak{q} \mid \mathfrak{p}) \xrightarrow{\pi_{\mathfrak{q}}} \mathrm{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q})) \longrightarrow 1, \tag{2.4}$$

and $|I(\mathfrak{q} \mid \mathfrak{p})| = e_{\mathfrak{p}}[\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]_i$*, where* $[\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]_i$ *denotes the inseparable degree of* $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$.

2. *Now assume further that* $\kappa(\mathfrak{p})$ *is perfect. Then* $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ *is Galois, and the short exact sequence 2.4 becomes*

$$1 \longrightarrow I(\mathfrak{q} \mid \mathfrak{p}) \longrightarrow D(\mathfrak{q} \mid \mathfrak{p}) \xrightarrow{\pi_{\mathfrak{q}}} \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \longrightarrow 1. \tag{2.5}$$

Furthermore, we have that $|I(\mathfrak{q} \mid \mathfrak{p})| = e_{\mathfrak{p}}$*, and*

$$\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \cong D(\mathfrak{q} \mid \mathfrak{p})/I(\mathfrak{q} \mid \mathfrak{p}).$$

Proof. 1. This is immediate from the relevant definitions.

2. We saw in Proposition 2.2.7 that $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is normal; it is separable since it is a finite extension and $\kappa(\mathfrak{p})$ is perfect. Therefore $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is Galois and $\mathrm{Aut}_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{q})) = \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$. Finally, since $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is separable, the inseparable degree $[\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]_i = 1$. The isomorphism follows immediately from the short exact sequence.

□

The next Lemma is the counterpart to Lemma 2.2.6 for the case of inertia groups.

Lemma 2.2.10. *For every* $g \in G$ *we have*

$$I({}^g\mathfrak{q} \mid \mathfrak{p}) = {}^gI(\mathfrak{q} \mid \mathfrak{p}).$$

Proof. Let $\sigma \in I({}^g\mathfrak{q} \mid \mathfrak{p})$. Then by definition,

$$\sigma b \equiv b \pmod{{}^g\mathfrak{p}}, \text{ for every } b \in B. \tag{2.6}$$

So let $b' \in B$ be arbitrary. Since $g(B) = B$, we have $g(b') \in B$ and according to 2.6 we have

$$\sigma(g(b')) \equiv g(b') \pmod{{}^g\mathfrak{p}} \iff \sigma(g(b')) - g(b') = g(a)$$

for some $a \in \mathfrak{p}$. Applying g^{-1} to each side, we get

$$(g^{-1}\sigma g)(b') - b' = a \in \mathfrak{p} \iff (g^{-1}\sigma g)b' \equiv b' \pmod{\mathfrak{p}}$$

which shows that $g^{-1}\sigma g \in I(\mathfrak{q} \mid \mathfrak{p})$, or equivalently,

$$\sigma \in gI(\mathfrak{q} \mid \mathfrak{p})g^{-1} = {}^gI(\mathfrak{q} \mid \mathfrak{p})$$

which establishes the containment $I({}^g\mathfrak{q} \mid \mathfrak{p}) \subseteq {}^gI(\mathfrak{q} \mid \mathfrak{p})$.

Now assume conversely that $\sigma \in {}^{g}I(\mathfrak{q} \mid \mathfrak{p})$. This means that $\sigma = g\tau g^{-1}$ for some $\tau \in I(\mathfrak{q} \mid \mathfrak{p})$. Now let $b \in B$ be arbitrary. We have

$$\left(g^{-1}\sigma\right) b = (\tau g^{-1})(b) = \tau\left(g^{-1}(b)\right).$$

But now $g^{-1}(b) \in B$ for all $b \in B$, thus

$$\left(g^{-1}\sigma\right) b = \tau\left(g^{-1}(b)\right) \equiv g^{-1}(b) \pmod{\mathfrak{p}} \iff \left(g^{-1}\sigma\right)(b) - g^{-1}(b) = a$$

for some $a \in \mathfrak{p}$. Applying g to each side, we see that

$$\sigma(b) - b = g(a) \in {}^{g}\mathfrak{p} \iff \sigma \in I({}^{g}\mathfrak{q} \mid \mathfrak{p}).$$

This establishes the second containment ${}^{g}I(\mathfrak{q} \mid \mathfrak{p})$ and the desired equality. □

2.2.3 Ramification in an intermediate extension

Assume $AKLBG$, and fix a subgroup $H \leq G$ of G. Let L^H denote the **fixed field of H in** L, and let B^H denote the **integral closure of A in L^H**. Then there are two more equivalent descriptions of B^H: it equals the intersection $B \cap L^H$, and it is also the subring of B fixed (pointwise) by H.

Taking a slight stylistic departure from the previous subsection, let $\mathfrak{p} \in \operatorname{spec}(B)$, and define $\mathfrak{p}_H := \mathfrak{p} \cap B^H \equiv \mathfrak{p} \cap L^H$. (By the same convention, $\mathfrak{p}_G = \mathfrak{p} \cap B^G = \mathfrak{p} \cap A \equiv \mathfrak{p} \cap K$). Then $L/L^H/K$ is a tower of finite separable extensions, $B/B^H/A$ is a tower of Dedekind extensions, and $\mathfrak{p} \mid \mathfrak{p}_H \mid \mathfrak{p}_G$ is a tower of primes. The relationship is illustrated in Figure 2.1.

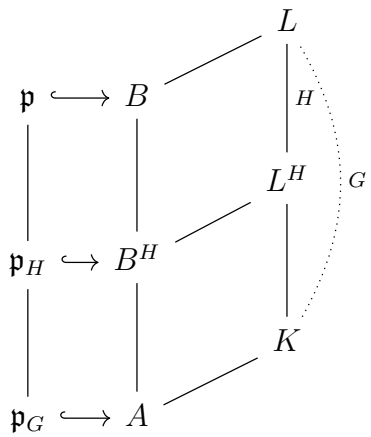


Figure 2.1: A tower of finite separable field extensions, Dedekind domains, and primes.

Lemma 2.2.11. *We have*

$$D(\mathfrak{p} \mid \mathfrak{p}_H) = D(\mathfrak{p} \mid \mathfrak{p}_G) \cap H, \text{ and}$$
$$I(\mathfrak{p} \mid \mathfrak{p}_H) = I(\mathfrak{p} \mid \mathfrak{p}_G) \cap H.$$

Proof. This follows by an immediate application of the definitions. □

Recall that ${}^g\mathfrak{p}$ denotes the image of $\mathfrak{p}$ under the action of $g \in G$ on $\mathbb{P}_L(\mathfrak{p}_G)$. Let

$$ {}^g\mathfrak{p}_H := {}^g\mathfrak{p} \cap B^H \equiv {}^g\mathfrak{p} \cap L^H. $$

Then for each $g \in G$ we have that ${}^g\mathfrak{p}_G = \mathfrak{p}_G$ and that ${}^g\mathfrak{p} \mid {}^g\mathfrak{p}_H \mid \mathfrak{p}_G$.

Corollary 2.2.12. *For every $g \in G$ we have*

$$ D({}^g\mathfrak{p} \mid {}^g\mathfrak{p}_H) = D({}^g\mathfrak{p} \mid \mathfrak{p}_G) \cap H = {}^g D(\mathfrak{p} \mid \mathfrak{p}_G) \cap H, \text{ and} $$

$$ I({}^g\mathfrak{p} \mid {}^g\mathfrak{p}_H) = I({}^g\mathfrak{p} \mid \mathfrak{p}_G) \cap H = {}^g I(\mathfrak{p} \mid \mathfrak{p}_G) \cap H. $$

Proof. We have ${}^g\mathfrak{p} \mid {}^g\mathfrak{p}_H \mid \mathfrak{p}_G$, and the first equality in each statement follows from Lemma 2.2.11. The equalities $D({}^g\mathfrak{p} \mid \mathfrak{p}_G) \cap H = {}^g D(\mathfrak{p} \mid \mathfrak{p}_G) \cap H$ and $I({}^g\mathfrak{p} \mid \mathfrak{p}_G) \cap H = {}^g I(\mathfrak{p} \mid \mathfrak{p}_G) \cap H$ follow immediately from Lemmas 2.2.6 and 2.2.10 respectively. □

Lemma 2.2.13. *Let $D := D(\mathfrak{p} \mid \mathfrak{p}_G)$. We have an equality and a bijection*

$$ \mathbb{P}_{L^H}(\mathfrak{p}_G) = \{{}^g\mathfrak{p}_H : g \in G\} \leftrightarrows H\backslash G/D, $$

where $H\backslash G/D$ is the double coset space.

Proof. For the equality, let $\mathfrak{q} \in \mathbb{P}_{L^H}(\mathfrak{p}_G)$. Then $\mathfrak{q} \cap K = \mathfrak{p}_G$. There is some $\mathfrak{Q} \in \mathbb{P}_L(\mathfrak{q})$; notice that in fact $\mathfrak{Q} \in \mathbb{P}_L(\mathfrak{p}_G)$ since

$$ \mathfrak{Q} \cap K = \left(\mathfrak{Q} \cap L^H\right) \cap K = \mathfrak{q} \cap K = \mathfrak{p}_G. $$

By G-transitivity on $\mathbb{P}_L(\mathfrak{p}_G)$, there is some $g \in G$ with ${}^g\mathfrak{p} = \mathfrak{Q}$. But then

$$ \mathfrak{q} = \mathfrak{Q} \cap L^H = {}^g\mathfrak{p} \cap L^H = {}^g\mathfrak{p}_H, $$

which proves $\mathbb{P}_{L^H}(\mathfrak{p}_G) \subseteq \{{}^g\mathfrak{p}_H : g \in G\}$.

Conversely, let $g \in G$ be arbitrary. Then ${}^g\mathfrak{p}_H \in \operatorname{spec}\left(B^H\right)$ and

$$ {}^g\mathfrak{p}_H \cap K = \left({}^g\mathfrak{p} \cap L^H\right) \cap K = {}^g\mathfrak{p} \cap K = \mathfrak{p}_G $$

which shows ${}^g\mathfrak{p}_H \in \mathbb{P}_{L^H}(\mathfrak{p}_G)$ and establishes the equality.

Now we define

$$ \begin{aligned} \psi : \ H\backslash G/D &\longrightarrow \{{}^g\mathfrak{p}_H : g \in G\} \\ HgD &\longmapsto {}^g\mathfrak{p}_H, \end{aligned} $$

and claim that ψ is a well-defined bijection.

To see that ψ is well-defined, suppose $Hg_1D = Hg_2D$ for some $g_1, g_2 \in G$. Notice that in particular we have $g_1 = hg_2\tau$ for some $h \in H$ and $\tau \in D$. Then we have

$$ \begin{aligned} {}^{g_1}\mathfrak{p}_H &= {}^{(hg_2\tau)}\mathfrak{p}_H \\ &= {}^{hg_2}({}^{\tau}\mathfrak{p}_H) \\ &= {}^{hg_2}\left({}^{\tau}\mathfrak{p} \cap L^H\right) \\ &= {}^{hg_2}\left(\mathfrak{p} \cap L^H\right) \\ &= {}^{hg_2}\mathfrak{p}_H \\ &= {}^{h}\left({}^{g_2}\mathfrak{p}_H\right). \end{aligned} $$

But now ${}^{g_2}\mathfrak{p}_H \subset B^H$ and $h\,|_{B^H} = \mathrm{Id}_{B^H}$, so ${}^{h}\left({}^{g_2}\mathfrak{p}_H\right) = {}^{g_2}\mathfrak{p}_H$ which proves ${}^{g_1}\mathfrak{p}_H = {}^{g_2}\mathfrak{p}_H$, hence ψ is well-defined.

By looking at the definition, it is clear that ψ is surjective. So to show that ψ is injective, suppose that ${}^{g_1}\mathfrak{p}_H = {}^{g_2}\mathfrak{p}_H$ for some $g_1, g_2 \in G$. Since double cosets partition any double coset space, in order to show that $Hg_1D = Hg_2D$, it suffices to show that $Hg_1D \cap Hg_2D \neq \emptyset$. We will show that $g_1 \in Hg_1D \cap Hg_2D$. It is clear that $g_1 \in Hg_1D$. Now, H acts transitively on $\mathbb{P}_L\left({}^{g_1}\mathfrak{p}_H\right) = \mathbb{P}_L\left({}^{g_2}\mathfrak{p}_H\right)$. Thus since ${}^{g_1}\mathfrak{p}, {}^{g_2}\mathfrak{p} \in \mathbb{P}_L\left({}^{g_1}\mathfrak{p}_H\right) = \mathbb{P}_L\left({}^{g_2}\mathfrak{p}_H\right)$ there is some $h \in H$ with

$$\begin{aligned} {}^{hg_2}\mathfrak{p} = {}^{g_1}\mathfrak{p} &\iff {}^{g_1^{-1}hg_2}\mathfrak{p} = \mathfrak{p} \\ &\iff g_1^{-1}hg_2 = \tau \in D \\ &\iff g_1 = hg_2\tau^{-1} \in Hg_2D. \end{aligned}$$

Therefore $Hg_1D = Hg_2D$ which proves that ψ is injective and we are done. □

Corollary 2.2.14. *Let $I := I\left(\mathfrak{p} \mid \mathfrak{p}_G\right)$. For every $g \in G$ we have*

$$e({}^{g}\mathfrak{p}_H \mid \mathfrak{p}_G) = \left[{}^{g}I : {}^{g}I \cap H\right].$$

Proof. Let $g \in G$. We have the tower of primes ${}^{g}\mathfrak{p} \mid {}^{g}\mathfrak{p}_H \mid \mathfrak{p}_G$, so by Proposition 2.2.2 we have

$$e({}^{g}\mathfrak{p} \mid \mathfrak{p}_G) = e({}^{g}\mathfrak{p} \mid {}^{g}\mathfrak{p}_H)e({}^{g}\mathfrak{p}_H \mid \mathfrak{p}_G).$$

Solving for $e({}^{g}\mathfrak{p}_H \mid \mathfrak{p}_G)$ and applying Corollaries 2.2.9 and 2.2.12 we see that

$$\begin{aligned} e({}^{g}\mathfrak{p}_H \mid \mathfrak{p}_G) &= \frac{e({}^{g}\mathfrak{p} \mid \mathfrak{p}_G)}{e({}^{g}\mathfrak{p} \mid {}^{g}\mathfrak{p}_H)} \\ &= \frac{\left|I\left({}^{g}\mathfrak{p} \mid \mathfrak{p}_G\right)\right|}{\left|I\left({}^{g}\mathfrak{p} \mid {}^{g}\mathfrak{p}_H\right)\right|} \\ &= \left[I\left({}^{g}\mathfrak{p} \mid \mathfrak{p}_G\right) : I\left({}^{g}\mathfrak{p} \mid {}^{g}\mathfrak{p}_H\right)\right] \\ &= \left[{}^{g}I : {}^{g}I \cap H\right]. \end{aligned}$$

□

By combining Lemma 2.2.13 and Corollary 2.2.14, we get the following:

Corollary 2.2.15. *We have that*

$$\left\{e(\mathfrak{q} \mid \mathfrak{p}_G) : \mathfrak{q} \in \mathbb{P}_{L^H}\left(\mathfrak{p}_G\right)\right\} = \left\{\left[{}^{g}I : {}^{g}I \cap H\right] : g \in G\right\}.$$

2.3 Application: exceptional values and periodic points in $\mathbb{Q}$

For this section, fix a positive integer n. We recall some old notation and introduce some new:

- $A_0 = \mathbb{Q}[t]$, and $K_0 = \mathbb{Q}(t)$;

- $\Phi_n(x)$ is the n-th dynatomic polynomial;
- $\Phi_{n,c}(x)$ is the n-th dynatomic polynomial specialized at c;
- L_0 and $L_{0,c}$ are the respective splitting fields of Φ_n over K_0 and $\Phi_{n,c}$ over $\mathbb{Q}$;
- $G = \mathrm{Gal}(L_0/K_0)$ and $G_c = \mathrm{Gal}(L_{0,c}/\mathbb{Q})$;
- Z and Z_c are the respective (geometric) zero sets of Φ_n and $\Phi_{n,c}$;
- $K_0' := \frac{K_0[x]}{(\Phi_n(x))} \cong K_0(\alpha)$ for some $\alpha \in Z$;
- let B_0 and A_0' denote the respective **integral closures** of A_0 in L_0 and K_0';
- $D_n = \{c \in \mathbb{Q} : \Phi_{n,c}(x) \text{ is inseparable}\}$;
- Fix $c \in \mathbb{Q}$ and let $\mathfrak{p} := (t-c) \in \mathrm{spec}(A_0)$ denote the corresponding **prime of** A_0.

Our first application is Corollary 2.3.7 which shows that whenever $c \in \mathbb{Q} - D_n$, then G_c embeds in G as a decomposition group. First we need to establish several preliminary results.

Lemma 2.3.1. *The following hold:*

(1) $Z \subset B_0$*;*

(2) For every $\mathfrak{P} \in \mathbb{P}_{L_0}(\mathfrak{p})$*, we have*

$$\Phi_n(x) \pmod{\mathfrak{P}} = \Phi_n(x) \pmod{\mathfrak{p}} = \Phi_{n,c}(x) \in \mathbb{Q}[x].$$

In particular, $\Phi_{n,c}(x)$ *splits completely in* $\kappa(\mathfrak{P})$*, and consequently* $L_{0,c} \subseteq \kappa(\mathfrak{P})$.

Proof. (1) By construction, $Z \subset L_0$. But since $\Phi_n(x) \in A_0[x]$ and Φ_n is monic in x, every $\alpha \in Z$ is integral over A_0.

(2) By $\Phi_n(x) \pmod{\mathfrak{P}}$ we mean the image of $\Phi_n(x)$ under the map $B_0[x] \twoheadrightarrow \kappa(\mathfrak{P})[x]$ which reduces each coefficient of Φ_n modulo $\mathfrak{P}$, and $\Phi_n(x) \pmod{\mathfrak{p}}$ similarly denotes the image of Φ_n under $A_0[x] \twoheadrightarrow \kappa(\mathfrak{p})[x]$. Then the first equality follows from the fact that the diagram

$$\begin{array}{ccc} B_0[x] & \twoheadrightarrow & \kappa(\mathfrak{P})[x] \\ \uparrow & & \uparrow \\ A_0[x] & \twoheadrightarrow & \kappa(\mathfrak{p})[x] \end{array}$$

commutes.

For the second equality, we should keep in mind that $\Phi_n(x) \in A_0[x] = (\mathbb{Q}[t])[x]$, so that the coefficients of $\Phi_n(x)$ are polynomials in t over $\mathbb{Q}$. But for a given coefficient $a(t) \in A_0$ of $\Phi_n(x)$, we know that $a(t) \pmod{\mathfrak{p}} = a(t) \pmod{(t-c)} = a(c) \in \mathbb{Q}$.

As $Z \subset B_0$, we have a complete splitting

$$\Phi_n(x) = (x - \alpha_1) \dots (x - \alpha_{nr}) \in B_0[x].$$

But then

$$\begin{aligned}\Phi_{n,c}(x) &= \Phi_n(x) \pmod{\mathfrak{P}} \\ &= (x - \alpha_1 \pmod{\mathfrak{P}}) \dots (x - \alpha_{nr} \pmod{\mathfrak{P}}) \in \kappa(\mathfrak{P})[x],\end{aligned}$$

which shows that $\Phi_{n,c}(x)$ splits completely over $\kappa(\mathfrak{P})$.

□

Lemma 2.3.2. *Let F/K_0 be any finite separable extension, and let B denote the integral closure of A_0 in F. Then $\kappa(\mathfrak{p}) = \mathbb{Q}$, and for every $\mathfrak{P} \in \mathbb{P}_F(\mathfrak{p})$ the residue field extension $\kappa(\mathfrak{P})/\mathbb{Q}$ is Galois.*

Proof. Consider that

$$\kappa(\mathfrak{p}) = \mathbb{Q}[t]/(t - c) \cong \mathbb{Q}(c) = \mathbb{Q}.$$

Thus since $\kappa(\mathfrak{P})$ is a finite extension of the perfect field $\kappa(\mathfrak{p}) = \mathbb{Q}$, the extension is separable. We saw in Proposition 2.2.7 that the residue field extension is normal. □

Now let H be the **subgroup of G corresponding to** K_0'; that is, $H = \mathrm{Gal}(L_0/K_0')$. Define

$$\mathrm{core}_G(H) := \bigcap_{g \in G} {}^gH$$

and call it the **(normal) core of H in G**. We will also use the notation N_H for $\mathrm{core}_G(H)$. Then N_H is characterized by the following property: N_H is the largest normal subgroup of G contained in H.

Lemma 2.3.3. *Let $\mathfrak{P} \in \mathbb{P}_{L_0}(\mathfrak{p})$ and define $I := I(\mathfrak{P} \mid \mathfrak{p})$. Then the following are equivalent:*

(1) $\mathfrak{p}$ is unramified in A_0';

(2) ${}^gI \subseteq H$ for every $g \in G$;

(3) $I \subseteq {}^gH$ for every $g \in G$;

(4) $I \subseteq N_H$.

Proof. The equivalences (2) $\iff$ (3) $\iff$ (4) are immediate from the definitions, so we prove (1) $\iff$ (2).

Since we have separable residue field extensions (Lemma 2.3.2), we know that $\mathfrak{p}$ is unramified in A_0' if and only if $e(\mathfrak{q} \mid \mathfrak{p}) = 1$ for every $\mathfrak{q} \in \mathbb{P}_{K_0'}(\mathfrak{p})$. According to Lemma 2.2.13, $e(\mathfrak{q} \mid \mathfrak{p}) = 1$ for every $\mathfrak{q} \in \mathbb{P}_{K_0'}(\mathfrak{p})$ if and only if $e({}^g\mathfrak{P}_H \mid \mathfrak{p}) = 1$ for every $g \in G$ where $\mathfrak{P}_H = \mathfrak{P} \cap A_0'$. But in Corollary 2.2.14 we saw that $e({}^g\mathfrak{P}_H \mid \mathfrak{p}) = [{}^gI : {}^gI \cap H]$, so $\mathfrak{p}$ is unramified in A_0' if and only if

$$1 = [{}^gI : {}^gI \cap H] \iff {}^gI = {}^gI \cap H \iff {}^gI \subseteq H,$$

for every $g \in G$. □

Lemma 2.3.4. *We have that* $N_H = \mathrm{core}_G(H) = \{1\}$.

Proof. Let E denote the Galois closure of K_0'/K_0, i.e., E is the smallest Galois extension of K_0 containing K_0'. We begin by recalling a classical fact from Galois theory: we have $E = L_0$ since L_0 is the splitting field of $\Phi_n(x)$ over K_0, and $\Phi_n(x)$ is the minimal polynomial of the primitive element α for the extension $K_0' = K_0(\alpha)$.

Let $L_0^{N_H}$ denote the fixed field in L_0 of N_H. Notice that in order to show $N_H = \{1\}$, it is equivalent to show that $L_0 = L_0^{N_H}$; the containment $L_0^{N_H} \subseteq L_0$ holds by definition. As $N_H \trianglelefteq G$, the sub-extension $L_0^{N_H}/K_0$ is Galois. Furthermore, we have $N_H \leq H$ which implies $K_0' = L_0^H \subseteq L_0^{N_H}$ by the Galois correspondence. Thus $L_0^{N_H}$ is Galois over K_0 and contains K_0'. But L_0 is the Galois closure of K_0'/K_0, so we must have $L_0 \subseteq L_0^{N_H}$ as well. □

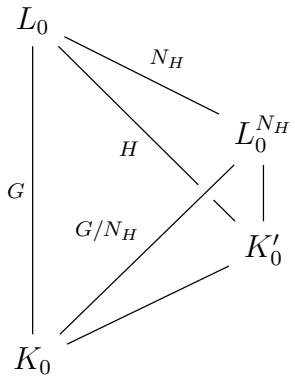


Figure 2.2: A Hasse diagram of field extensions together with associated Galois groups.

Corollary 2.3.5. *If* $c \in \mathbb{Q} - D_n$, *then* $\mathfrak{p}$ *is unramified in* B_0.

Proof. We start off with the claim that $\Phi_{n,c}(x)$ separable implies that $\mathfrak{p}$ is unramified in A_0'. Indeed,

$$0 \neq \mathrm{disc}(\Phi_{n,c}(x)) = \mathrm{disc}(\Phi_n(x) \pmod{\mathfrak{p}}) = \mathrm{disc}(\Phi_n(x)) \pmod{\mathfrak{p}}$$

so $\mathfrak{p}$ does not divide $\mathrm{disc}(\Phi_n(x))$. On the other hand, the discriminant $\mathrm{disc}(A_0'/A_0)$ divides $\mathrm{disc}(\Phi_n(x))$. Therefore $\mathfrak{p}$ cannot divide $\mathrm{disc}(A_0'/A_0)$, and $\mathfrak{p}$ is unramified in A_0'.

Having established that $\mathfrak{p}$ is unramified in A_0', Lemma 2.3.3 then shows that $I(\mathfrak{P} \mid \mathfrak{p}) \subseteq N_H$ for every $\mathfrak{P} \in \mathbb{P}_{L_0}(\mathfrak{p})$. But in Lemma 2.3.4, we saw that $N_H = \{1\}$. Thus,

$$e(\mathfrak{P} \mid \mathfrak{p}) = |I(\mathfrak{P} \mid \mathfrak{p})| = 1$$

for every $\mathfrak{P} \in \mathbb{P}_{L_0}(\mathfrak{p})$, which proves $\mathfrak{p}$ is unramified in B_0. □

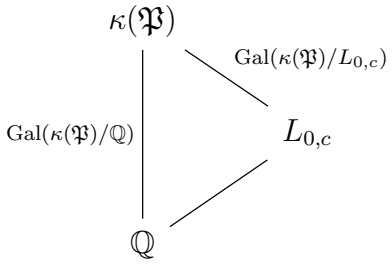
The next Theorem and its proof constitute a retelling of Proposition 2.3 and its proof from [9].

Theorem 2.3.6. *Let* $c \in \mathbb{Q} - D_n$, *fix* $\mathfrak{P} \in \mathbb{P}_{L_0}(\mathfrak{p})$, *and let* D *denote the decomposition group* $D(\mathfrak{P} \mid \mathfrak{p})$. *Then there is an isomorphism of group actions* $D \cong G_c$ *where* D *acts on* Z *and* G_c *acts on* Z_c.

Proof. By Lemma 2.3.2, the residue field extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p}) = \kappa(\mathfrak{P})/\mathbb{Q}$ is Galois. Given $\alpha \in B_0$, we let $\bar{\alpha} := \alpha \pmod{\mathfrak{P}}$ denote its image in $\kappa(\mathfrak{P})$. Similar to our notation for decomposition, let I denote the inertia group $I(\mathfrak{P} \mid \mathfrak{p})$. Recall (see Corollary 2.2.9) that we have the surjective group homomorphism $\pi_{\mathfrak{P}} : D \to \mathrm{Gal}(\kappa(\mathfrak{P})/\mathbb{Q})$ with kernel I sending σ to $\bar{\sigma}$, where $\bar{\sigma}(\bar{\alpha}) = \overline{\sigma(\alpha)}$. By Corollary 2.3.5, our assumption that $c \in \mathbb{Q} - D_n$ implies that $\mathfrak{p}$ is unramified in B_0, and so I is the trivial group. Therefore $\pi_{\mathfrak{P}}$ induces an isomorphism

$$\mathrm{Gal}(\kappa(\mathfrak{P})/\mathbb{Q}) \cong D/I = D.$$

We saw in Lemma 2.3.1 that $L_{0,c} \subseteq \kappa(\mathfrak{P})$. Now we will show that $L_{0,c} = \kappa(\mathfrak{P})$, by showing that the Galois sub-extension $\kappa(\mathfrak{p})/L_{0,c}$ of $\kappa(\mathfrak{P})/\mathbb{Q}$ has trivial Galois group.



As we saw in Lemma 2.3.1, if $\alpha \in Z$ then $\bar{\alpha} \in Z_c$. Furthermore, since $\Phi_{n,c}(x)$ is separable, if α_i and α_j are distinct roots of $\Phi_n(x)$, then $\bar{\alpha}_i \neq \bar{\alpha}_j$. We therefore get that reduction modulo $\mathfrak{P}$ is an injective map from Z to Z_c. But since $\Phi_{n,c}(x)$ is separable and $\deg \Phi_{n,c}(x) = \deg \Phi_n(x)$, we get that $|Z_c| = |Z|$. In particular this implies that reduction modulo $\mathfrak{P}$ is a bijection $Z \leftrightarrows Z_c$. Notice that $L_{0,c}$ can be written as $L_{0,c} = \mathbb{Q}(\bar{\alpha}_1, \ldots, \bar{\alpha}_{nr})$.

So now, let $\tau \in \mathrm{Gal}(\kappa(\mathfrak{P})/\mathbb{Q})$ be arbitrary. As $\pi_{\mathfrak{P}}$ is surjective, there is some $\sigma \in D$ with $\tau = \pi_{\mathfrak{P}}(\sigma) = \bar{\sigma}$. Since $\tau|_{L_{0,c}} = \mathrm{Id}_{L_{0,c}}$ we have that $\tau(\bar{\alpha}_i) = \bar{\alpha}_i$ for every $i \in [nr]$. So for each $i \in [nr]$ we see that $\bar{\alpha}_i = \tau(\bar{\alpha}_i) = \bar{\sigma}(\bar{\alpha}_i) = \overline{\sigma(\alpha_i)}$. But now, $\alpha_i \in Z$ and $\sigma \in D \leq G$ imply that $\sigma(\alpha_i) \in Z$, and since reduction modulo $\mathfrak{P}$ gives an injection $Z \hookrightarrow Z_c$, we are forced to conclude that $\sigma(\alpha_i) = \alpha_i$ for every $i \in [nr]$. The Galois action on roots of an irreducible polynomial is faithful, so we see that in fact $\sigma = 1$. This implies $\tau = \pi_{\mathfrak{P}}(\sigma) = \pi_{\mathfrak{P}}(1) = 1$, which shows that $\mathrm{Gal}(\kappa(\mathfrak{P})/L_{0,c})$ is trivial, or equivalently that $\kappa(\mathfrak{P}) = L_{0,c}$. Consequently,

$$D \cong \mathrm{Gal}(\kappa(\mathfrak{P})/L_{0,c}) = \mathrm{Gal}(L_{0,c}/\mathbb{Q}) = G_c$$

which shows that we have the required group isomorphism.

Finally notice that for all $i, j \in [nr]$ we have $\sigma(x_i) = x_j$ if and only if $\bar{\sigma}(\bar{\alpha}_i) = \bar{\alpha}_j$, so this isomorphism of groups is in fact an isomorphism of group actions. □

Corollary 2.3.7. *If $c \in \mathbb{Q} - D_n$, then $G_c \cong D(\mathfrak{P} \mid \mathfrak{p}) \leq G$ for any $\mathfrak{P} \in \mathbb{P}_{L_0}(\mathfrak{p})$.*

Recall from Section 1.4 that

$$E_n = \{c \in \mathbb{Q} - D_n : G_c \lneq G\}$$

is the n-th exceptional set.

Theorem 2.3.8. *Let $c \in \mathbb{Q} - D_n$. If $\mathrm{Per}_n(f_c; \mathbb{Q})$ is non-empty, then $c \in E_n$.*

Proof. Let $c \in \mathbb{Q} - D_n$. Notice that if $\alpha \in \mathrm{Per}_n(f_c; \mathbb{Q}) \subseteq Z_c \cap \mathbb{Q}$, then the natural action of G_c on Z_c is intransitive. Indeed, for every $n \geq 1$ we have $|Z_c| \geq 2$ and so there is some $\beta \in Z_c$ with $\beta \neq \alpha$. But then $g\alpha = \alpha \neq \beta$ for every $g \in G_c = \mathrm{Gal}(L_{0,c}/\mathbb{Q})$, so the action is intransitive.

We argue by the contrapositive: suppose that $c \notin E_n$, or equivalently that $G_c = G$. As $G_c = G$ we see that $Z, Z_c \in G_c$–**Set**, and the isomorphism from Theorem 2.3.6 shows that Z and Z_c are isomorphic as G_c–sets. Since $Z = Z(\Phi_n)$ and $\Phi_n(x) \in K_0[x]$ is irreducible, the natural action of $G = G_c$ on Z is transitive. Therefore G_c acts on Z_c transitively since Z and Z_c are isomorphic G_c–sets, and by the previous paragraph $\mathrm{Per}_n(f_c; \mathbb{Q})$ must be empty. □

Thus in order to show that for a given n, there are at most finitely many $c \in \mathbb{Q}$ for which f_c has a point in $\mathbb{Q}$ of period n, it suffices to show that E_n is finite. Our goal then is to show that E_n is finite for every $n \geq 10$.

Chapter 3

Curves, Function Fields, and Genus

To properly discuss dynatomic modular curves and their genera, we first need to review some basic notions from algebraic geometry.

3.1 Galois theory of curves

There is an equivalence of categories between functions fields and curves. We summarize several of the key results following [16, Chapter 1], and [18, Lectures 18,19].

3.1.1 Function fields, places, and primes

Fix a perfect field $\mathbb{F}$.

Definition 3.1.1. (1) A **function field over** $\mathbb{F}$ is any finitely generated field extension $L/\mathbb{F}$ with transcendence degree 1 over $\mathbb{F}$ and for which L is algebraically closed in $\mathbb{F}$. Let $\mathcal{F}_{\mathbb{F}}$ denote the **category of all function fields over** $\mathbb{F}$ with morphisms given by field homomorphisms which restrict to the identity on $\mathbb{F}$.

(2) Let $L \in \mathcal{F}_{\mathbb{F}}$. A **place of** $L/\mathbb{F}$ is the unique maximal ideal P of some discrete valuation ring $\mathcal{O}_P$ of $L/\mathbb{F}$. We let $\mathbb{P}_L$ denote the **set of all places of** $L/\mathbb{F}$.

(3) Let $L \in \mathcal{F}_{\mathbb{F}}$, and let $P \in \mathbb{P}_L$. The **residue field of** P is the field $\mathcal{O}_P/P$.

For a function field $L \in \mathcal{F}_{\mathbb{F}}$ and a place $P \in \mathbb{P}_L$, one can show that $\mathbb{F} \subseteq \mathcal{O}_P/P$. We define $\deg P$, the **degree of** P, by $\deg P := [\mathcal{O}_P/P : \mathbb{F}]$. In fact, we have that $\deg P < \infty$ for every $P \in \mathbb{P}_L$. If $\deg P = 1$ (so that $\mathcal{O}_P/P = \mathbb{F}$), then we say that P is a **rational place**. Notice that if $\mathbb{F}$ is algebraically closed, then every $P \in \mathbb{P}_L$ is rational.

Now we consider the special case of the rational function field over $\bar{\mathbb{Q}}$: let $\mathbb{F} = \bar{\mathbb{Q}}$ and consider $K := \bar{\mathbb{Q}}(t) \in \mathcal{F}_{\bar{\mathbb{Q}}}$, where t is transcendental over $\bar{\mathbb{Q}}$.

For every monic irreducible polynomial $q(t) \in \bar{\mathbb{Q}}[t]$, there is an associated discrete valuation ring $\left(\mathcal{O}_{P_q}, P_q\right)$ of $K/\bar{\mathbb{Q}}$ given as follows:

$$\mathcal{O}_{P_q} \equiv \mathcal{O}_q := \left\{ \frac{f(t)}{g(t)} \in K : q(t) \nmid g(t) \right\}, \quad P_q := \left\{ \frac{f(t)}{g(t)} \in \mathcal{O}_q : q(t) \mid f(t) \right\}.$$

Any place of the form P_q (where $q(t) \in \bar{\mathbb{Q}}[t]$ is a monic irreducible polynomial) is called a **finite place of** $K/\bar{\mathbb{Q}}$. One can show that $P_q = (q(t))\mathcal{O}_q$ so that $q(t)$ generates P_q; we say that $q(t)$ is a **uniformizer/local parameter/prime element** for P_q. Furthermore, there is an isomorphism

$$\mathcal{O}_q/P_q \cong \frac{\bar{\mathbb{Q}}[t]}{(q(t))},$$

which in particular shows that $\deg P_q = \deg q(t)$.

But now, since $\bar{\mathbb{Q}}$ is algebraically closed every place of $K/\bar{\mathbb{Q}}$ (and in particular every finite place) is rational. Thus we must have $\deg q(t) = 1$ so that $q(t) = t - c$ for some $c \in \bar{\mathbb{Q}}$. We will use the shorthands $\mathcal{O}_c$ and P_c for $\mathcal{O}_{t-c}$ and P_{t-c} respectively. To summarize, every finite place of $K/\bar{\mathbb{Q}}$ has the form P_c for some $c \in \bar{\mathbb{Q}}$, and there is a bijection

$$\{\text{finite places } P \in \mathbb{P}_K\} \leftrightarrows \operatorname{spec}\left(\bar{\mathbb{Q}}[t]\right)$$

given by $P_c \mapsto (t - c)$.

There is another distinguished discrete valuation ring $(\mathcal{O}_{P_\infty}, P_\infty)$ of $K/\bar{\mathbb{Q}}$ given by

$$\mathcal{O}_{P_\infty} \equiv \mathcal{O}_\infty := \left\{\frac{f(t)}{g(t)} \in K : \deg f \leq \deg g\right\}, \quad P_\infty := \left\{\frac{f(t)}{g(t)} \in \mathcal{O}_\infty : \deg f < \deg g\right\}.$$

The place P_∞ is called the **infinite place of** $K/\bar{\mathbb{Q}}$. We have that $\frac{1}{t}$ is a uniformizer of P_∞, and $\deg P_\infty = 1$.

Theorem 3.1.2. *We have that* $\mathbb{P}_{\bar{\mathbb{Q}}(t)} = \{P_\infty\} \sqcup \left\{P_c : c \in \bar{\mathbb{Q}}\right\}$.

Proof. Combine the fact that $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}$ has only rational places with [16, Theorem 1.2.2.]. □

3.1.2 Curves

Fix a perfect field $\mathbb{F}$.

Definition 3.1.3. (1) A **curve over** $\mathbb{F}$ is any non-singular projective variety C of dimension one which is defined over $\mathbb{F}$.

(2) Let $\mathcal{C}_\mathbb{F}$ denote the **category of all curves over** $\mathbb{F}$ with morphisms given by non-constant morphisms of varieties defined over $\mathbb{F}$.

(3) For a curve $C \in \mathcal{C}_\mathbb{F}$, we let $\mathbb{F}(C)$ denote the **function field of** C.

(4) For a curve $C \in \mathcal{C}_\mathbb{F}$, we let $C(\mathbb{F})$ denote the **set of all** $\mathbb{F}$**-rational points of** C.

It is a fact that $\mathbb{F}(C) \in \mathcal{F}_\mathbb{F}$ for every curve $C \in \mathcal{C}_\mathbb{F}$, so we have a way of associating a function field to each curve. To a function field $L \in \mathcal{F}_\mathbb{F}$, we would like to associate a curve $C \in \mathcal{C}_\mathbb{F}$ for which $\mathbb{F}(C) = L$. First we recall the notion of an abstract curve.

Assume that $\mathbb{F}$ is algebraically closed, and let $L \in \mathcal{F}_\mathbb{F}$. Define $X \equiv X_L := \mathbb{P}_L$, the set of all places of $L/\mathbb{F}$. For any $U \subseteq X$, the **ring of regular functions on** U is

$$\mathcal{O}_X(U) \equiv \mathcal{O}(U) := \bigcap_{P \in U} \mathcal{O}_P.$$

It is a fact that X has a topology whose closed sets are all finite subsets of X together with X itself. Then $X \equiv X_L$ is the **abstract curve associated to** $L \in \mathcal{F}_{\mathbb{F}}$.

Let each of X and Y be an abstract curve, or a projective variety. A **morphism of abstract curves or projective varieties** is any continuous map $\phi : X \to Y$ for which the following property holds: for every open subset $U \subseteq Y$ and every $f \in \mathcal{O}_Y(U)$ we have that $f \circ \phi \in \mathcal{O}_X\left(\phi^{-1}(U)\right)$. Thus we have a category whose objects are abstract curves and projective varieties with morphisms as above.

Theorem 3.1.4. *(1) Let $C \in \mathcal{C}_{\mathbb{F}}$, and let $X = X_{\mathbb{F}(C)}$ be the abstract curve associated to its function field $\mathbb{F}(C)$. Then C and X are isomorphic.*

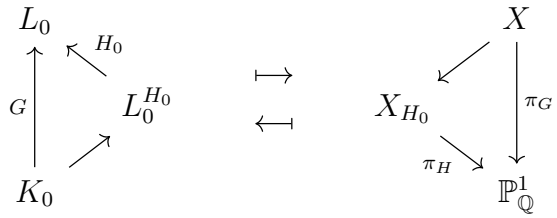
(2) For every function field $L \in \mathcal{F}_{\mathbb{F}}$, there is some curve $C \in \mathcal{C}_{\mathbb{F}}$ such that the abstract curve X_L is isomorphic to C.

Proof. Statements (1) and (2) appear as Theorem 18.10. and Theorem 18.13. of [18]. □

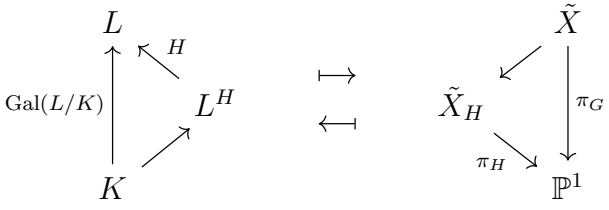
We therefore have all the ingredients for the categorical equivalence $\mathcal{F}_{\mathbb{F}} \simeq \mathcal{C}_{\mathbb{F}}$ when $\mathbb{F}$ is algebraically closed. Even if $\mathbb{F}$ is merely assumed to be perfect (and not necessarily algebraically closed) we still have the equivalence $\mathcal{F}_{\mathbb{F}} \simeq \mathcal{C}_{\mathbb{F}}$. In this case though, the construction of the curve associated to a function field is different.

Theorem 3.1.5 ([18, Theorem 19.2])**.** *For any perfect field $\mathbb{F}$, the categories $\mathcal{C}_{\mathbb{F}}$ and $\mathcal{F}_{\mathbb{F}}$ are contravariantly equivalent via the functor sending $C \in \mathcal{C}_{\mathbb{F}}$ to its function field $\mathbb{F}(C)$, and sending a morphism $\phi : C_1 \to C_2$ to $\phi^* : \mathbb{F}(C_2) \to \mathbb{F}(C_1)$ given by $\phi^*(f) = f \circ \phi$.*

Recall that $K_0 = \mathbb{Q}(t)$, that L_0 is the splitting field of $\Phi_n(x)$ over K_0, and that $L_0^{H_0}$ denotes the fixed field of H_0 in L_0 for every subgroup $H_0 \leq G = \mathrm{Gal}(L_0/K_0)$. Then we claim that K_0, L_0, and $L_0^{H_0}$ are objects of $\mathcal{F}_{\mathbb{Q}}$ for every $H_0 \leq G$. Thus there are curves X, X_{H_0}, and Y in $\mathcal{C}_{\mathbb{Q}}$ corresponding to L_0, $L_0^{H_0}$, and K_0 respectively. It is not difficult to see that the curve Y corresponding to $K_0 = \mathbb{Q}(t)$ is $\mathbb{P}^1_{\mathbb{Q}}$, the **projective line defined over** $\mathbb{Q}$. Moreover, it is a standard fact that the curve X_{H_0} corresponding to $L_0^{H_0}$ is the quotient curve X/H_0 whose points are H_0-orbits under the action of H_0 on X. We therefore have equivalent diagrams



Now let $K := \bar{\mathbb{Q}}(t)$, let L denote the splitting field of $\Phi_n(x)$ over K, and for any subgroup $H \leq \mathrm{Gal}(L/K)$, we let L^H denote the fixed field of H in L. Now that we are working over $\bar{\mathbb{Q}}$, each of K, L, and L^H is an object of $\mathcal{F}_{\bar{\mathbb{Q}}}$ and we get corresponding curves $\mathbb{P}^1$, $\tilde{X}$, and $\tilde{X}_H$ in $\mathcal{C}_{\bar{\mathbb{Q}}}$ and equivalent diagrams



Definition 3.1.6. A **dynatomic modular curve** is any curve of the form X_{H_0} where H_0 is a subgroup of the dynatomic Galois group G, or a curve of the form $\tilde{X}_H$ where H is any subgroup of $\mathrm{Gal}(L/K)$.

3.2 Genus of a curve

Let $\mathbb{F}$ be a fixed perfect field. For a curve $C \in \mathcal{C}_{\mathbb{F}}$, let $g(C)$ denote the **genus of** C. The genus is an important birational invariant of C (meaning that two curves have the same genus if and only if they are birationally equivalent). A useful first property of the genus is the following:

Proposition 3.2.1. *The following hold:*

(1) Let $C_1, C_2 \in \mathcal{C}_{\bar{\mathbb{Q}}}$. If there is a dominant morphism $\psi : C_1 \to C_2$, then $g(C_1) \geq g(C_2)$.

(2) Let H_0 be any proper subgroup of G and M any maximal subgroup of G containing H_0. Then $g(X_{H_0}) \geq g(X_M)$.

Proof. (1) See Example 2.5.4. of [7, Chapter IV].

(2) The subgroup relation $H_0 \leq M$ induces an inclusion of fixed fields $L_0^M \hookrightarrow L_0^{H_0}$ which in turn induces a dominant morphism $X_{H_0} \to X_M$, and the bound $g(X_{H_0}) \geq g(X_M)$ follows from (1).

□

For a subgroup $H_0 \leq G$, we will interchangeably use the notations $g(X_{H_0})$ and $g(L_0^{H_0})$ to denote the **genus of the dynatomic modular curve** X_{H_0}. Similarly, for any subgroup $H \leq \mathrm{Gal}(L/K)$, we will interchangeably use $g(\tilde{X}_H)$ and $g(L^H)$ to denote the **genus of the dynatomic modular curve** $\tilde{X}_H$.

A breakthrough achievement in arithmetic geometry was the 1983 proof of the Mordell Conjecture by Faltings.

Theorem 3.2.2 (Faltings' Theorem [4])**.** *Let $C \in \mathcal{C}_{\mathbb{Q}}$. If $g(C) \geq 2$, then the set $C(\mathbb{Q})$ is finite.*

The Riemann-Hurwitz genus formula 3.1 will be our primary tool for calculating (or at least bounding from below) genus. The next result shows that "genus can be calculated geometrically."

Proposition 3.2.3 ([8, Proposition 2.2])**.** *Let $\mathbb{F}$ be any field such that $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$, and let $L_{\mathbb{F}}$ be the splitting field of $\Phi_n(x)$ over $\mathbb{F}(t)$. Then there is an isomorphism*

$$\iota : \mathrm{Gal}(L_{\mathbb{F}}/\mathbb{F}(t)) \to G = \mathrm{Gal}(L_0/\mathbb{Q}(t))$$

with the following property: if we let $H_0 := \iota(H)$ for a subgroup $H \leq \mathrm{Gal}(L_{\mathbb{F}}/\mathbb{F}(t))$, then $g\left(L_{\mathbb{F}}^H\right) = g\left(L_0^{H_0}\right)$.

Now let $\mathbb{F} = \bar{\mathbb{Q}}$. Then the Proposition gives an isomorphism

$$\iota : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_0/K_0) = G$$

such that for any subgroup $H \leq \mathrm{Gal}(L/K)$, the function fields L^H and $L_0^{H_0}$ have the same genus where $H_0 = \iota(H) \leq G$.

3.2.1 The Riemann-Hurwitz genus formula

We recall that $K = \bar{\mathbb{Q}}(t)$, and that L is the splitting field of $\Phi_n(x)$ over K. We will now use G to denote $\mathrm{Gal}(L/K)$. For a subgroup $H \leq G$, we let L^H denote the fixed field of H in L. Recall that $\mathbb{P}_K$ denotes the set of all places of $K/\bar{\mathbb{Q}}$, and also recall that according to Theorem 3.1.2, we have $\mathbb{P}_K = \{P_\infty\} \sqcup \{P_c : c \in \bar{\mathbb{Q}}\}$, where P_∞ is the infinite place of $K/\bar{\mathbb{Q}}$ and P_c is the finite place of $K/\bar{\mathbb{Q}}$ corresponding to $(t-c) \in \mathrm{spec}(A)$, where $A = \bar{\mathbb{Q}}[t]$.

Let K' denote the primitive K-extension

$$K' = \frac{K[x]}{(\Phi_n(x))} \cong K(\alpha)$$

for some $\alpha \in Z = \{\alpha \in L : \Phi_n(\alpha) = 0\}$. Let $\mathbb{P}$ denote the **set of all places of $K/\bar{\mathbb{Q}}$ which ramify in K'**.

Finally, for a place $P \in \mathbb{P}_K$ and any intermediate field $K \leq \mathbb{F} \leq L$, let $\mathbb{P}_{\mathbb{F}}(P)$ denote **the set of all places of $\mathbb{F}/\bar{\mathbb{Q}}$ lying over P**. We can now state a formula for calculating the genera of dynatomic modular curves in terms of ramification data.

Theorem 3.2.4 ([16, Corollary 3.5.6.])**.** *For any subgroup $H \leq G$ we have*

$$2g(L^H) - 2 = (-2)[G : H] + \sum_{P \in \mathbb{P}} \sum_{Q|P} (e(Q \mid P) - 1), \tag{3.1}$$

where the second sum runs over all places $Q \in \mathbb{P}_{L^H}(P)$, and $e(Q \mid P)$ is the ramification index of $Q \mid P$.

By Proposition 3.2.3, we also have that

$$2g(L_0^{H_0}) - 2 = (-2)[G : H] + \sum_{P \in \mathbb{P}} \sum_{Q|P} (e(Q \mid P) - 1),$$

where H_0 is the subgroup of $\mathrm{Gal}(L_0/K_0)$ which corresponds to H under the isomorphism $G \cong \mathrm{Gal}(L_0/K_0)$. Enabled by this genus preserving isomorphism, we will no longer use as much caution in distinguishing $\mathrm{Gal}(L/K)$ from $\mathrm{Gal}(L_0/K_0)$.

3.2.2 Rational points and exceptional values

Recall that $D_n = \{c \in \mathbb{Q} : \Phi_{n,c} \text{ is inseparable}\}$. Recall also that we showed in Corollary 2.3.7 that $c \in \mathbb{Q} - D_n$ implies that $G_c \leq G$. The goal of this thesis is to show that for $n = 11$ and every $n \geq 13$, there are at most finitely $c \in \mathbb{Q}$ for which $f_c(x) = x^2 + c$ has some point in $\mathbb{Q}$ of period n. We saw in Theorem 2.3.8 that for this goal, it suffices to show that the exceptional set

$$E_n = \{c \in \mathbb{Q} - D_n : G_c \lneq G\}$$

is finite for every $n \geq 5$. We now see an important connection between exceptional values $c \in E_n$ and rational points on dynatomic modular curves X_H.

Theorem 3.2.5. *Let $c \in \mathbb{Q} - D_n$. Then $c \in E_n$ if and only if $c \in \pi_H(X_H(\mathbb{Q}))$ for some proper subgroup $H \lneq G$.*

Proof. For a proof, see the proof of Proposition 3.3.1 and Proposition 3.3.5 of [15]. □

Proposition 3.2.6. *Let n be a fixed positive integer. If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.*

Proof. We first claim that to show E_n is finite, it suffices to show that $g(X_H) \geq 2$ for every proper subgroup $H \lneq G$. Indeed, if this holds then $X_H(\mathbb{Q})$ is finite for every $H \lneq G$ by Faltings' Theorem 3.2.2. But then $\pi_H(X_H(\mathbb{Q}))$ must be finite (since the morphism π_H sends finite sets to finite sets), and by Theorem 3.2.5 this implies that E_n is finite.

Now assume that $g(X_M) \geq 2$ for every maximal subgroup M of G. If $H \lneq G$ is an arbitrary proper subgroup, then there is some maximal subgroup M of G with $H \leq M$. By Proposition 3.2.1, we get that $g(X_H) \geq g(X_M) \geq 2$, and therefore E_n is finite by the previous paragraph. □

Chapter 4

Dynatomic Galois Groups as Semi-Direct Products

4.1 Abstract Semi-Direct Products

The dynatomic Galois group G is isomorphic to a certain semi-direct product, and this semi-direct product description is foundational to our ultimate goal. First we review some of the basics of abstract semi-direct products.

4.1.1 External

Let Γ and N be two groups such that there exists $\varphi : \Gamma \to \mathrm{Aut}\,(N)$ a group homomorphism. We will write $\varphi_\gamma \in \mathrm{Aut}\,(N)$ for the image of $\gamma \in \Gamma$ under φ, and ${}^\gamma n$ in place of $\varphi_\gamma(n) \in N$. Then $(\gamma, n) \mapsto {}^\gamma n$ defines a (left) action of Γ on N which is compatible with the group structure of N. We define a group $N \rtimes \Gamma$ as follows:

- $N \rtimes \Gamma := N \times \Gamma$ (as sets);
- $(n_1, \gamma_1)(n_2, \gamma_2) := (n_1(\varphi_{\gamma_1}(n_2)), \gamma_1\gamma_2) = (n_1\,({}^{\gamma_1}n_2)\,, \gamma_1\gamma_2)$;
- $(1, 1) = 1 \in N \rtimes \Gamma$;
- $(n, \gamma)^{-1} = \left({}^{\gamma^{-1}}n^{-1}, \gamma^{-1}\right)$.

Then $N \rtimes \Gamma$ is a group called the **(external) semi-direct product** of N and Γ. Note that the structure of $N \rtimes \Gamma$ depends on the choice of homomorphism $\varphi : \Gamma \to \mathrm{Aut}\,(N)$, so the most precise notational choice would reflect this dependence as $N \rtimes_\varphi \Gamma$. Frequently though, φ is understood from context hence the sloppier $N \rtimes \Gamma$.

4.1.2 Internal

The proof of the following Lemma involves only the relevant definitions, and is therefore omitted.

Lemma 4.1.1. *Let C be a group, A and B subgroups of C and suppose that $A \trianglelefteq C$ is normal. Then the following are equivalent:*

1. *$C = AB$ and $A \cap B = \{1\}$.*
2. *Every $c \in C$ can be uniquely expressed as $c = ab$ for some $a \in A$ and $b \in B$.*
3. *Every $c \in C$ can be uniquely expressed as $c = ba$ for some $a \in A$ and $b \in B$.*
4. *If $\pi : C \to C/A$ denotes the natrual quotient and $\iota : B \to C$ the natural inclusion homomorphisms, then $\pi \circ \iota : B \to C/A$ is an isomorphism.*
5. *There is a homomorphism $C \to B$ which restricts to the identity on B and whose kernel is A.*
6. *There is a split short exact sequence*

$$1 \longrightarrow A \longrightarrow C \longrightarrow B \longrightarrow 1.$$

If any of these equivalent conditions is satisfied, then we say that C is an **(internal) semi-direct product** of A and B.

4.1.3 Equivalent notions

Lemma 4.1.2. *Suppose we are given that $N \rtimes \Gamma$ is an (external) semi-direct product of groups N and Γ.*

1. *$N \rtimes \Gamma$ has subgroups*

$$N^* := \{(n, 1) : n \in N\},$$
$$\Gamma^* := \{(1, \gamma) : \gamma \in \Gamma\},$$

   which are naturally isomorphic to N and Γ respectively.

2. *We have that $N^* \trianglelefteq N \rtimes \Gamma$, and that each $(n, \gamma) \in N \rtimes \Gamma$ can be expressed as $n^*\gamma^*$ for unique elements $n^* \in N^*$ and $\gamma^* \in \Gamma^*$.*

Proof. 1. Apply the definitions.

2. N^* is normal in $N \rtimes \Gamma$ if and only if for every $(n, \gamma) \in N \rtimes \Gamma$ we have

$$(n, \gamma)N^*(n, \gamma)^{-1} \subseteq N^*$$

So let $(m, 1) \in N^*$. Then

$$\begin{aligned}(n, \gamma)(m, 1)(n, \gamma)^{-1} &= (n\,({}^{\gamma}m), \gamma)\left({}^{\gamma^{-1}}n^{-1}, \gamma^{-1}\right) \\ &= (n({}^{\gamma}m)^{\gamma}\left({}^{\gamma^{-1}}n^{-1}\right), \gamma\gamma^{-1}) \\ &= (n({}^{\gamma}m)n^{-1}, 1) \in N^*,\end{aligned}$$

which proves N^* is normal in $N \rtimes \Gamma$.

Now let $(n, \gamma) \in N \rtimes \Gamma$ be arbitrary. According to the group law of $N \rtimes \Gamma$, we see that $(n, \gamma) = (n, 1)(1, \gamma)$. We claim that this is the unique way of expressing (n, γ) as an element of $N^*\Gamma^*$. Indeed, suppose there are elements $m^* \in N^*$ and $\beta^* \in \Gamma^*$ for which $(n, \gamma) = m^*\beta^*$. By the definitions of N^* and Γ^*, there are elements $m \in N$ and $\beta \in \Gamma$ for which $m^* = (m, 1)$ and $\beta^* = (1, \beta)$. Again, by the group law

$$(n, \gamma) = m^*\beta^* = (m, 1)(1, \beta) = (m, \beta)$$

which holds if and only if $m = n$ and $\beta = \gamma$. This proves that the decomposition $(n, \gamma) = (n, 1)(1, \gamma)$ is unique.

□

By the Lemmas, we see that the *external* semi-direct product $N \rtimes \Gamma$ is an *internal* semi-direct product of N^* and Γ^*. The converse also holds, as we show in the next result.

Lemma 4.1.3. *Let C be a group which is an (internal) semi-direct product of subgroups A and B with $A \trianglelefteq C$. For each $c \in C$, let $\varphi_c \in \mathrm{Aut}\,(C)$ denote the conjugation-by-c automorphism defined by $\varphi_c(x) = cxc^{-1}$ for every $x \in C$. Then the map*

$$\begin{aligned} \varphi : \ B &\longrightarrow \mathrm{Aut}\,(A) \\ b &\longmapsto \varphi_b \end{aligned}$$

is a group homomorphism and $C = AB \cong A \rtimes_\varphi B$.

Proof. That φ is a group homomorphism follows immediately from normality of A.

We define a map

$$\begin{aligned} \Psi : \ AB &\longrightarrow A \rtimes_\varphi B \\ ab &\longmapsto (a, b) \end{aligned}$$

and claim that it's an isomorphism; it is clearly bijective. To see that Ψ is a group homomorphism, we compute directly:

$$\begin{aligned} \Psi((a_1b_1)(a_2b_2)) &= \Psi((a_1b_1a_2b_1^{-1})(b_1b_2)) \\ &= (a_1b_1a_2b_1^{-1}, b_1b_2) \\ &= (a_1 \left({}^{b_1}a_2\right), b_1b_2) \\ &= (a_1, b_1)(a_2, b_2) \\ &= \Psi(a_1b_1)\Psi(a_2b_2). \end{aligned}$$

□

Lemmas 4.1.2 and 4.1.3 show that (upon making suitable choices), internal and external semi-direct products are the same.

Lemma 4.1.4. *Let G be any finite group, N a normal subgroup of G, Γ the quotient group G/N, and $\pi : G \to \Gamma$ the quotient map. If π is split, then G is isomorphic to a certain semi-direct product $N \rtimes \Gamma$.*

Proof. Let $\iota : \Gamma \to G$ be some splitting of $\pi : G \to \Gamma$. This means that $\iota : \Gamma \to G$ is a group homomorphism with the property that $\pi \circ \iota = \mathrm{Id}_\Gamma$. Notice that this implies ι is injective, for if $\gamma_1 = \gamma_2$, then

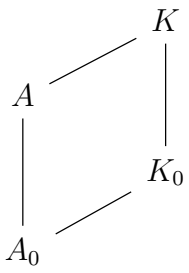
$$\gamma_1 = \pi(\iota(\gamma_1)) = \pi(\iota(\gamma_2)) = \gamma_2.$$

Thus $\iota : \Gamma \to G$ is an inclusion, and Γ is (isomorphic to) some subgroup of G. By condition (4) of Lemma 4.1.1, we have that G is an internal semi-direct product $G = N\Gamma$, and then by Lemma 4.1.3, we see that $G \cong N \rtimes \Gamma$ where the Γ-action on N (by automorphisms of N) is conjugation. □

4.2 The Dynatomic Setting

Here we apply the results of the previous section to symmetry groups of dynatomic polynomials. First we set our notation and recall a few basic facts:

- Let t be transcendental over $\mathbb{C}$.
- Define A_0 to be the Dedekind domain $\mathbb{Q}[t]$, and define $K_0 := \mathrm{Frac}(A_0) = \mathbb{Q}(t)$, the **rational function field over** $\mathbb{Q}$.
- Similarly, we define A to be the Dedekind domain $\bar{\mathbb{Q}}[t]$, and $K := \mathrm{Frac}(A) = \bar{\mathbb{Q}}(t)$, **the rational function field over** $\bar{\mathbb{Q}}$. We have a diagram of inclusions



  where the inclusions run in the direction of increasing height.
- Let $f(x) := x^2 + t \in A_0[x]$ denote the **generic quadratic polynomial over** $\mathbb{Q}$.
- For each positive integer n, let $\Phi_n(x)$ denote the **n-th dynatomic polynomial of** $f(x)$. We have that:
  - $\Phi_n(x) \in A_0[x]$ is monic in x;
  - $\Phi_n(x)$ is geometrically irreducible;
  - $\deg \Phi_n(x) = nr$ for some positive integer r.

- Let L (respectively L_0) denote the **splitting field** of $\Phi_n(x)$ over K (respectively K_0).
- By geometric irreducibility of $\Phi_n(x)$, the extension L/K is Galois; let $G := \mathrm{Gal}(L/K)$ be the **n-th (generic) dynatomic Galois group (of $f(x)$)**.
- Let $Z \equiv Z(\Phi_n(x)) := \{\alpha \in L : \Phi_n(\alpha) = 0\}$ denote the **(geometric) zero set of** $\Phi_n(x)$. We saw in Corollary 1.3.4 that
$$Z = \bigsqcup_{i=1}^{r} A_i$$
where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ for some $\alpha_i \in L$, for each $i \in [r]$. Each A_i has precisely n elements and is called the **i-th f-orbit of** Z, or simply an **f-orbit**.
- Let $\Sigma := \mathrm{Sym}\,(Z) \cong S_{nr}$.
- Let $\Omega := \{A_1, \ldots, A_r\}$, the **set of all f-orbits**.
- Let $\Gamma := \mathrm{Sym}\,(\Omega)$. We will frequently identify Γ and S_r (and their natural actions on Ω and $[r]$ respectively) under the isomorphism induced by the natural bijection $A_i \leftrightarrows i$.
- Let $C := \mathrm{Cent}_\Sigma(f)$ denote the **centralizer of f in Σ**.
- Let $N := (\mathbb{Z}/n)^r$.

4.2.1 C as a semi-direct product

Let $\sigma \in C$ be arbitrary. For each $i \in [r]$, we have
$$\sigma(f^j(\alpha_i)) = f^j(\sigma(\alpha_i))$$
for every $j \in \mathbb{Z}/n$. Thus, $\sigma(A_i)$ is some other f-orbit; the unique such f-orbit containing $\sigma(\alpha_i)$. We therefore have a well-defined permutation $\gamma \in \Gamma$ associated to σ given by
$$\gamma(A_i) \equiv A_{\gamma(i)} := \sigma(A_i)$$
and a resulting permutation representation
$$\begin{aligned} \phi : \ C &\longrightarrow \Gamma \\ \sigma &\longmapsto \gamma = [A_i \mapsto \sigma(A_i)] \end{aligned}$$

Proposition 4.2.1. *The following hold:*

1. *Let $\gamma \in \Gamma$. We define a map $\sigma : Z \to Z$ by*
$$\sigma(f^j(\alpha_i)) := f^j(\alpha_{\gamma(i)}). \tag{4.1}$$
Then $\sigma \in C$ and $\phi(\sigma) = \gamma$, so that ϕ is surjective.

2. *For $\eta \in \ker(\phi)$ and $i \in [r]$, let $j_i \in \mathbb{Z}/n$ denoe the well-defined exponent for which $\eta(\alpha_i) = f^{j_i}(\alpha_i) \in A_i$. Then the map*

$$\begin{aligned} \psi : \ker(\phi) &\longrightarrow N \\ \eta &\longmapsto (j_1, \ldots, j_r) \end{aligned}$$

is an isomorphism of groups.

3. *We have a short exact sequence of groups*

$$1 \longrightarrow N \longrightarrow C \xrightarrow{\phi} \Gamma \longrightarrow 1$$

and thus an isomorphism

$$\begin{aligned} \bar{\phi} : C/N &\xrightarrow{\cong} \Gamma \\ \sigma N &\longmapsto \phi(\sigma) \end{aligned}$$

which makes the diagram

$$\begin{array}{ccc} C & \xrightarrow{\pi} & C/N \\ & {\scriptstyle\phi}\searrow \quad \swarrow{\scriptstyle\bar{\phi}} & \\ & \Gamma & \end{array}$$

commute.

4. *We define a map $\iota : \Gamma \to C$ as follows: for $\gamma \in \Gamma$, let $\iota(\gamma) := \sigma$ (the same σ from 4.1), so that*

$$\iota(\gamma)(f^j(\alpha_i)) = f^j(\alpha_{\gamma(i)}).$$

Then $i : \Gamma \to C$ is a splitting of $\phi : C \to \Gamma$.

Proof. 1. Let $\gamma \in \Gamma$ and $\sigma : Z \to Z$ be as defined in 4.1. Suppose that

$$\sigma(f^j(\alpha_i)) = \sigma(f^k(\alpha_\ell))$$

for some $j, k \in \mathbb{Z}/n$ and some $i, \ell \in [r]$. By the decomposition $Z = \sqcup_{i=1}^r A_i$, we immediately see that $i = \ell$ and $j = k$, so that σ is injective, hence also surjective (as $\sigma : Z \to Z$ and Z is finite), and thus $\sigma \in \Sigma = \mathrm{Sym}(Z)$. Furthermore,

$$\begin{aligned} (\sigma f)(f^j(\alpha_i)) &= \sigma(f^{j+1}(\alpha_i)) \\ &= f^{j+1}(\alpha_{\gamma(i)}) \\ &= f(f^j(\alpha_{\gamma(i)})) \\ &= f(\sigma(f^j(\alpha_i))) \\ &= (f\sigma)(f^j(\alpha_i)), \end{aligned}$$

thus $\sigma f = f\sigma$ so that $\sigma \in C$. Finally, $\sigma(\alpha_i) = \alpha_{\gamma(i)} \in A_{\gamma(i)} \equiv \gamma(A_i)$, so $\phi(\sigma) = \gamma$ by definition.

2. For each $\eta \in \ker(\phi)$, we have $\eta(A_i) = A_i$, and thus $\eta\,|_{A_i} \in \mathrm{Sym}(A_i)$ for every $i \in [r]$. If j_i is the exponent for which $\eta(\alpha_i) = f^{j_i}(\alpha_i) \in A_i$, then j_i uniquely determines $\eta\,|_{A_i}$ since
$$\eta(f^j(\alpha_i)) = f^j(\eta(\alpha_i)) = f^j(f^{j_i}(\alpha_i)) = f^{j+j_i}(\alpha_i),$$
for each $j \in \mathbb{Z}/n$. It follows that η is uniquely determined by $(j_1, \ldots, j_r) \in N$, and we get an injective group homomorphism
$$\begin{aligned} \psi :\ \ker(\phi) &\longrightarrow N \\ \eta &\longmapsto (j_1, \ldots, j_r). \end{aligned}$$
To see that ψ is surjective, given an arbitrary $(j_1, \ldots, j_r) \in N$, define $\eta : Z \to Z$ by
$$\eta(f^j(\alpha_i)) = f^{j+j_i}(\alpha_i).$$
It's routine to check that $\eta \in \ker(\phi)$, and it's clear by definition that $\psi(\eta) = (j_1, \ldots, j_r) \in N$.

3. Follows immediately from 1. and 2.

4. $\iota : \Gamma \to C$ is a group homomorphism since for $\gamma_1, \gamma_2 \in \Gamma$ we have
$$\begin{aligned} \iota(\gamma_1\gamma_2)(f^j(\alpha_i)) &= f^j(\alpha_{(\gamma_1\gamma_2)(i)}) \\ &= f^j(\alpha_{\gamma_1(\gamma_2(i))}) \\ &= \iota(\gamma_1)(f^j(\alpha_{\gamma_2(i)})) \\ &= \iota(\gamma_1)(\iota(\gamma_2)(f^j(\alpha_i))) \\ &= (\iota(\gamma_1)\iota(\gamma_2))(f^j(\alpha_i)). \end{aligned}$$
Recall that by definition $\iota(\gamma) = \sigma$, where σ is the element of C defined in 4.1 and shown to satisfy $\phi(\sigma) = \gamma$. Thus,
$$(\phi \circ \iota)(\gamma) = \phi(\iota(\gamma)) = \phi(\sigma) = \gamma$$
and we get that $\phi \circ \iota = \mathrm{Id}_\Gamma$, which is precisely what it means for ι to split ϕ.

□

We will henceforth identify C/N and Γ along the isomorphism
$$\begin{aligned} \bar{\phi} :\ C/N &\longrightarrow \Gamma \\ \sigma N &\longmapsto \phi(\sigma) \end{aligned}$$

After making this identification, the quotient map
$$\begin{aligned} \pi :\ C &\longrightarrow C/N \\ \sigma &\longmapsto \sigma N \end{aligned}$$

becomes

$$\begin{aligned} \phi : \ C &\longrightarrow \Gamma \\ \sigma &\longmapsto \phi(\sigma) \end{aligned}$$

so that π and ϕ are identified as well.

Corollary 4.2.2. *We have*

$$C \cong N \rtimes \Gamma.$$

To be precise, C is isomorphic to the (external) semi-direct product $N \rtimes \Gamma$ where the Γ-action (by automorphisms) on N is conjugation in C.

Proof. We have that C is a finite group with subgroups (isomorphic to) N and Γ, and that $N \trianglelefteq C$. By the discussion above, $\Gamma \cong C/N$ and the quotient map $\pi : C \to C/N$ is just $\phi : C \to \Gamma$. We showed in Proposition 4.2.1 that $\iota : \Gamma \to C$ is a splitting of $\phi : C \to \Gamma$, so $\pi : C \to C/N$ is seen to split as well. By Lemma 4.1.4, we have that $C \cong N \rtimes \Gamma$ with the Γ-action on N as described above. □

4.2.2 Γ transitivity on N

$N = (\mathbb{Z}/n)^r$ is a free $(\mathbb{Z}/n)$-module with (standard) basis $\{e_1, \ldots, e_r\}$, where e_i is the r-tuple with 1 in position i and 0 everywhere else and is called the **i-th standard basis vector**.

Under the isomorphism $\psi : \ker(\phi) \cong N$, the i-th standard basis vector e_i corresponds to $f_i \in \ker(\phi)$ given by

$$f_i(f^j(\alpha_k)) := \begin{cases} f^{j+1}(\alpha_i), & \text{if } k = i; \\ f^j(\alpha_k), & \text{else.} \end{cases} \tag{4.2}$$

In other words, f_i acts as f on A_i and as Id_{A_k} on every A_k with $k \neq i$, or more succinctly,

$$f_i \mid_{A_k} = \begin{cases} f, & \text{if } k = i; \\ \mathrm{Id}_{A_k}, & \text{else.} \end{cases} \tag{4.3}$$

In the semi-direct product description $C \cong N \rtimes \Gamma$, the group Γ acts on N by conjugation in C. We want to explore this Γ-action on the standard basis $\{e_1, \ldots, e_r\} \equiv \{f_1, \ldots, f_r\}$. To this end, let $\gamma \in \Gamma$ be arbitrary. As is common, we will identify γ with its image $\iota(\gamma) \in C$. Let

$i \in [r]$ and $f^j(\alpha_k) \in Z$ be arbitrary. Then

$$\begin{aligned}
({}^{\gamma}f_i)\left(f^j(\alpha_k)\right) &= (\gamma f_i \gamma^{-1})\left(f^j(\alpha_k)\right) \\
&= (\gamma f_i)\left(f^j(\alpha_{\gamma^{-1}(k)})\right) \\
&= \gamma\left(\begin{cases} f^{j+1}(\alpha_i), & \text{if } \gamma^{-1}(k) = i; \\ f^j(\alpha_{\gamma^{-1}(k)}), & \text{else,} \end{cases}\right) \\
&= \begin{cases} f^{j+1}(\alpha_{\gamma(i)}), & \text{if } \gamma^{-1}(k) = i; \\ f^j(\alpha_{\gamma(\gamma^{-1}(k))}), & \text{else,} \end{cases} \\
&= \begin{cases} f^{j+1}(\alpha_{\gamma(i)}), & \text{if } \gamma(i) = k; \\ f^j(\alpha_k), & \text{else.} \end{cases}
\end{aligned} \tag{4.4}$$

By definition, the standard basis vector $f_{\gamma(i)}$ acts on Z according to

$$f_{\gamma(i)}\left(f^j(\alpha_k)\right) = \begin{cases} f^{j+1}(\alpha_{\gamma(i)}), & \text{if } \gamma(i) = k; \\ f^j(\alpha_k), & \text{else.} \end{cases} \tag{4.5}$$

By comparing 4.4 and 4.5, we see that $({}^{\gamma}f_i)\left(f^j(\alpha_k)\right) = f_{\gamma(i)}\left(f^j(\alpha_k)\right)$ for every $j \in \mathbb{Z}/n$ and every $k \in [r]$. We conclude that

$${}^{\gamma}f_i = \gamma f_i \gamma^{-1} = f_{\gamma(i)} \in N.$$

We have therefore proved the following:

Lemma 4.2.3. *For every $i \in [r]$ and every $\gamma \in \Gamma$ we have that*

$${}^{\gamma}f_i \equiv \gamma f_i \gamma^{-1} = f_{\gamma(i)}.$$

In particular, the Γ-action on N by conjugation in C is transitive on the standard basis $\{e_1, \ldots, e_r\} \equiv \{f_1, \ldots, f_r\}$ for N.

4.2.3 G as a semi-direct product

Recall that $G = \mathrm{Gal}(L/K)$ is the n-th (generic) dynatomic Galois group. We aim to show that $G \cong N \rtimes \Gamma$ by first showing that $G = C$ and then invoking Corollary 4.2.2.

Lemma 4.2.4. *We have an inclusion $G \hookrightarrow C$.*

Proof. Let $g \in G \leq \Sigma = \mathrm{Sym}\,(Z)$. Notice that $f(x) \in A_0[x] \subset K[x]$ implies that $f^m(x) \in A_0[x] \subset K[x]$ for every non-negative integer m. But now $g \in G = \mathrm{Gal}(L/K)$, so g acts as Id_K on K, and thus

$$g(f^m(\alpha)) = f^m(g(\alpha)), \text{ for every } m \in \mathbb{Z}_{\geq 0} \text{ and every } \alpha \in L.$$

In particular,

$$\begin{aligned}(gf)\left(f^j(\alpha_i)\right) &= g(f^{j+1}(\alpha_i)) \\ &= f(g\left(f^j(\alpha_i)\right)) \\ &= (fg)\left(f^j(\alpha_i)\right)\end{aligned}$$

for every $f^j(\alpha_i) \in Z$. This shows that $gf = fg \in \Sigma$, or equivalently that $g \in C$. □

We note that the Lemma and proof which follow are adaptations of Lemme 3 on page 65 of [2].

Lemma 4.2.5. *Let H be any subgroup of C for which $\pi(H) = \Gamma$. If there is some $g \in G$ such that ${}^g e_1 \in H$, then $H = C$.*

Proof. We first reduce the problem to showing that $N \subseteq H$. Indeed, let $\tau \in C$ be arbitrary. As $\phi(H) = \Gamma$, we can find some $h_0 \in H$ which satisfies

$$\phi(h_0) = \phi(\tau) \in \Gamma \quad \Longleftrightarrow \quad h_0^{-1}\tau \in \ker(\phi) = N.$$

If $N \subseteq H$, then $h_0^{-1}\tau \in H$ which implies $\tau \in h_0 H = H$. It therefore suffices to show that $N \subseteq H$.

Lemma 4.2.3 shows that Γ acts transitively on $\{e_1, \ldots, e_r\}$ by conjugation, thus so does H. In particular, for every $i \in [r]$, there is some $h_i \in H$ with $e_i = {}^{h_i}({}^g e_1)$. But then

$$e_i = {}^{h_i}({}^g e_1) = h_i({}^g e_1)h_i^{-1} \in H$$

since we are conjugating the element $({}^g e_1) \in H$ by $h_i \in H$. It follows that $\{e_1, \ldots, e_r\} \subseteq H$ and therefore $N \subseteq H$. □

Corollary 4.2.6. *We have that*

$$G = C \cong N \rtimes \Gamma = (\mathbb{Z}/n)^r \rtimes S_r.$$

Proof. Of course we have that $e_1 \in G$, so we are done (by Lemma 4.2.5) if we know that G maps onto Γ; this was proved by Bousch in [2]. □

Chapter 5

Ramification of Dynatomic Polynomials

In this section we look at the ramification theory of dynatomic polynomials and wherever ramification occurs, we provide a description of the corresponding inertia subgroup of G.

5.1 Ramification

5.1.1 Discriminants and resultants of dynatomic polynomials

Recall that $Z \equiv Z(\Phi_n(x)) := \{\alpha \in L : \Phi_n(\alpha) = 0\}$ denotes the **(geometric) zero set of** $\Phi_n(x)$. We saw that

$$Z = \bigsqcup_{i=1}^{r} A_i$$

where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ for some $\alpha_i \in L$, for each $i \in [r]$. Each A_i has precisely n elements and is called the i**-th** f**-orbit of** Z, or simply an f**-orbit**.

To each f-orbit A_i we associate the i**-th multiplier** $\omega_i := (f^n)'(\alpha_i)$ which is the formal x-derivative of the polynomial $f^n(x)$ evaluated at α_i. By the chain rule and our description of the orbit A_i, we have

$$\omega_i = (f^n)'(\alpha_i) = \prod_{k=0}^{n-1} f'(f^k(\alpha_i)) = \prod_{\alpha \in A_i} f'(\alpha).$$

On the other hand, $f(x) = x^2 + t$ so we know that $f'(x) = 2x$ and therefore

$$\omega_i = \prod_{\alpha \in A_i} f'(\alpha) = \prod_{\alpha \in A_i} 2\alpha = 2^n \prod_{\alpha \in A_i} \alpha.$$

The n**-th multiplier polynomial** is

$$\delta_n(x) := \prod_{i=1}^{r} (x - \omega_i) \in L_0[x].$$

For each positive integer m, allow $C_m(x)$ to denote the m**-th cyclotomic polynomial**

$$C_m(x) := \prod_{d|m} (x^d - 1)^{\mu(m/d)}.$$

For each divisor $d \mid n$ with $d \neq n$ we define

$$\Delta_{n,d} := \mathrm{Res}(C_{n/d}(x), \delta_d(x))$$

where $\mathrm{Res}(g_1(x), g_2(x))$ is the **resultant** of the polynomials $g_1(x)$ and $g_2(x)$.

Lastly, we define $\Delta_{n,n}$ according to the equation

$$\delta_n(1) = \Delta_{n,n} \prod_{\substack{d|n,\\ d<n}} \Delta_{n,d}$$

The objects $\Delta_{n,d}$ for divisors d of n were introduced by Morton and Vivaldi in [13] in their study of the discriminants and resultants of dynatomic polynomials. The following Theorem aggregates several results along these lines.

Theorem 5.1.1 (Morton and Vivaldi [13])**.** *The following hold:*

1. *For every positive integer n and every divisor d of n we have that $\Delta_{n,d} \in \mathbb{Z}[t]$.*
2. $\mathrm{disc}(\Phi_n(x)) = \pm(\Delta_{n,n}(t))^n \prod_{\substack{d|n,\\ d<n}} (\Delta_{n,d}(t))^{n-d}$.
3. *If $d \mid n$ and $d < n$, then*

$$\mathrm{Res}(\Phi_n(x), \Phi_d(x)) = \pm(\Delta_{n,d}(t))^d.$$

4. *Let $R_{n,d} := Z(\Delta_{n,d}(t)) \subset \overline{\mathbb{Q}}$. Then*
   (a) $|R_{n,d}| = \deg(\Delta_{n,d}(t))$.
   (b) *If d and e are distinct divisors of n, then $R_{n,d} \cap R_{n,e} = \emptyset$.*
   (c) *Let φ denote Euler's φ function, and define*

$$\nu(s) := \frac{1}{2} \sum_{d|s} \mu(s/d) 2^d$$

for each positive integer s. We have the formula

$$\deg(\Delta_{n,d}(t)) = \begin{cases} \nu(d)\varphi(n/d), & \text{if } d < n; \\ \nu(n) - \sum_{\substack{k|n,\\ k<n}} \nu(k)\varphi(n/k), & \text{if } d = n. \end{cases} \tag{5.1}$$

Table 5.1 presents examples of the invariants $\Delta_{n,d}$ for several small n. It is compiled from the data in Table 1 of [13].

n	d	$\Delta_{n,d}(t)$	$\deg(\Delta_{n,d}(t))$
1	1	$-1+4t$	1
2	1	$3+4t$	1
2	2	-1	0
3	1	$7+4t+16t^2$	2
3	3	$7+4t$	1
4	1	$5-8t+16t^2$	2
4	2	$-5-4t$	1
4	4	$135+108t+144t^2+64t^3$	3

n	d	$\deg(\Delta_{n,d}(t))$
5	1	4
5	5	11
6	1	2
6	2	2
6	3	3
6	6	20

Table 5.1: Some small $\Delta_{n,d}$ invariants and their degrees.

5.1.2 Ramification of places of K

Let K' denote the **primitive K-extension**

$$K' := \frac{K[x]}{(\Phi_n(x))} \cong K(\alpha)$$

for some $\alpha \in Z$, let B' denote the **integral closure** of A in K', and let

$$\mathbb{P} := \{\text{places } P \text{ of } K \text{ which ramify in } K'\}.$$

The utility of the polynomials $\Delta_{n,d}(t)$ is that their zero sets $R_{n,d}$ parameterize $\mathbb{P}$. To make this precise, we require some notation. Recall that P_∞ denotes the **infinite place** of K: that is, the place corresponding to the valuation $v_\infty(f/g) = \deg g - \deg f$ on K. For each $c \in \overline{\mathbb{Q}}$, we also let P_c denote the place corresponding to the prime $(t-c) \in \operatorname{spec}(A)$.

Theorem 5.1.2 (Morton [10])**.** *The following hold:*

1. $\mathbb{P} = \{P_\infty\} \sqcup \{P_c \mid c \in \sqcup_{d|n} R_{n,d}\}$;

2. *For each $P \in \mathbb{P}$, the factorization of PB' into places of B' is given by*

$$PB' = \begin{cases} \wp_1^2 \cdots \wp_{\nu(n)}^2, & \text{if } P = P_\infty; \\ \wp_1^{n/d} \cdots \wp_d^{n/d} \mathfrak{q}_1 \cdots \mathfrak{q}_{n(r-1)}, & \text{if } P = P_c \text{ with } c \in R_{n,d},\ d < n; \\ \wp_1^2 \cdots \wp_n^2 \mathfrak{q}_1 \cdots \mathfrak{q}_{n(r-2)} & \text{if } P = P_c \text{ with } c \in R_{n,n}. \end{cases} \tag{5.2}$$

   (Note that in each of the three cases above, the places are (in general) different even though we have used the same symbols to denote them.)

3. *$B' = A[\alpha]$, so that B' has integral power basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{nr-1}\}$.*

5.2 Inertia

Here we present a description of generators of inertia subgroups of G for places $P \in \mathbb{P}$ due to Krumm ([8]). First we require some notation.

Let Γ be a group and X any finite (left) Γ-set. We say that $\gamma \in \Gamma$ has **cycle-type** (ℓ, k) if the disjoint cycle decomposition of $\gamma \in \mathrm{Sym}(X)$ is a product of k many ℓ-cycles (ignoring fixed points).

Recall that for an intermediate extension F of L/K and a place P of K we have used the notation

$$\mathbb{P}_F(P) := \{\text{places } Q \text{ of } F \text{ lying over } P\}.$$

Proposition 5.2.1 (Krumm [8])**.** *Let $P \in \mathbb{P}$ and $Q \in \mathbb{P}_L(P)$. Let $I(Q \mid P)$ denote the inertia subgroup of $Q \mid P$. Then $I(Q \mid P)$ has a generator with cycle-type (ℓ, k) satisfying*

$$(\ell, k) = \begin{cases} \left(2, \frac{nr}{2}\right), & \text{if } P = P_\infty; \\ (2, n), & \text{if } P = P_c \text{ for } c \in R_{n,n}; \\ \left(\frac{n}{d}, d\right), & \text{if } P = P_c \text{ for } c \in R_{n,d} \text{ with } d < n. \end{cases} \tag{5.3}$$

(Here the cycle-type (ℓ, k) means the cycle-type of the generator of $I(Q \mid P)$ as an element of $\Sigma = \mathrm{Sym}(Z)$).

5.2.1 Identifying inertia subgroups

In this subsection we give a precise description of some inertia subgroups in terms of the semi-direct product description of $G = N \rtimes \Gamma = (\mathbb{Z}/n)^r \rtimes S_r$.

Let d be any divisor of n, let $c \in R_{n,d} = Z(\Delta_{n,d}(t)) \subset \bar{\mathbb{Q}}$, and fix a prime $\mathfrak{p} \in \mathbb{P}_L(P_c)$. Let I_d denote the **inertia subgroup** $I(\mathfrak{p} \mid P_c)$. We will prove that $I_d = \langle d \cdot e_j \rangle$ for some $j \in [r]$ where we recall that e_j is the j-th standard basis element for $N = (\mathbb{Z}/n)^r$ with 1 in coordinate j and 0 elsewhere.

By Theorem 5.1.1, we have that

$$\pm(\Delta_{n,d}(t))^d = \mathrm{Res}(\Phi_n(x), \Phi_d(x))$$

and so we get that

$$0 = \pm(\Delta_{n,d}(c))^d = \mathrm{Res}(\Phi_{n,c}(x), \Phi_{d,c}(x)).$$

Thus there is some $a \in \bar{\mathbb{Q}}$ for which

$$\Phi_{n,c}(a) = 0 = \Phi_{d,c}(a), \tag{5.4}$$

which in turn implies that

$$f_c^n(a) = a = f_c^d(a) \tag{5.5}$$

Now we introduce some notation: for $\beta \in B$, let $\overline{\beta} := \beta \pmod{\mathfrak{p}}$ denote the **reduction of β modulo $\mathfrak{p}$**, and for $h(x) \in B[x]$, let $\overline{h}(x)$ denote the **reduction modulo $\mathfrak{p}$ of** h: that is, the polynomial of $(B/\mathfrak{p})[x]$ obtained from $h(x)$ by reducing each coefficient modulo $\mathfrak{p}$. The next result is proved by using that reduction modulo $\mathfrak{p}$ is a ring homomorphism.

Lemma 5.2.2. *Let $\beta \in B$ and $h(x) \in B[x]$ be arbitrary. Then the following hold:*

1. $\overline{h(\beta)} = \overline{h}(\overline{\beta})$;
2. $\overline{h}^j(x) = \overline{h^j}(x)$ *for every* $j \in \mathbb{Z}_{\geq 0}$.

Now consider the extension of residue fields $(B/\mathfrak{p})/(A/P_c)$. Notice that

$$A/P_c = \frac{\bar{\mathbb{Q}}[t]}{(t-c)} \cong \bar{\mathbb{Q}}(c) = \bar{\mathbb{Q}}.$$

But now $B/\mathfrak{p}$ is a finite (hence algebraic) extension of the algebraically closed field $\bar{\mathbb{Q}} = A/P_c$, and so the only possibility is that $B/\mathfrak{p} = \bar{\mathbb{Q}} = (A/P_c)$.

Since the mod $\mathfrak{p}$ reduction map $B \twoheadrightarrow \bar{\mathbb{Q}}$ is surjective, there is some $\alpha \in B$ with $a = \overline{\alpha}$. Furthermore, Lemma 2.3.1 shows that $\Phi_{n,c}(x) = \overline{\Phi_n}(x)$ and $\Phi_{d,c}(x)\,\overline{\Phi_d}(x)$, and by the same argument given for Lemma 2.3.1 we also have that $f_c^n(x) = \overline{f}^n(x)$ and $f_c^d(x) = \overline{f}^d(x)$. With these identifications in mind, if we reduce each side of the equations 5.4 and 5.5 mod $\mathfrak{p}$, then we see that

$$\begin{cases} \overline{\Phi_n}(\overline{\alpha}) = 0 = \overline{\Phi_d}(\overline{\alpha}) \\ \overline{f}^n(\overline{\alpha}) = \overline{f^n(\alpha)} = \overline{\alpha} = \overline{f^d(\alpha)} = \overline{f}^d(\overline{\alpha}). \end{cases} \tag{5.6}$$

Now recall that $\Phi_n(x)$ splits completely in $B[x]$ as

$$\Phi_n(x) = \prod_{i=1}^{r} \left[(x-\alpha_i)(x-f(\alpha_i))\dots(x-f^{n-1}(\alpha_i))\right].$$

Therefore $\Phi_{n,c}(x) = \overline{\Phi_n}(x)$ splits completely in $\bar{\mathbb{Q}}[x]$ as

$$\overline{\Phi_n}(x) = \prod_{i=1}^{r} \left[(x-\overline{\alpha_i})(x-\overline{f}(\overline{\alpha_i}))\dots(x-\overline{f}^{n-1}(\overline{\alpha_i}))\right]. \tag{5.7}$$

Since $0 = \overline{\Phi_n}(\overline{\alpha})$, the above splitting shows that $\overline{\alpha} = \overline{f}^j(\overline{\alpha_\ell})$ for some $\ell \in [r]$ and some $j \in \mathbb{Z}/n$. After a possible reordering of the orbits and a cyclic shift of the elements within each orbit, we may assume that $\ell = 1$ and $j = 0$ so that $\overline{\alpha} = \overline{\alpha_1}$.

Lemma 5.2.3. *We have that*

$$(x-\overline{\alpha_1})(x-\overline{f}(\overline{\alpha_1}))\dots(x-\overline{f}^{n-1}(\overline{\alpha_1})) = \left((x-\overline{\alpha_1})(x-\overline{f}(\overline{\alpha_1}))\dots(x-\overline{f}^{d-1}(\overline{\alpha_1}))\right)^{n/d} \in \bar{\mathbb{Q}}[x].$$

Proof. By 5.6, we have that

$$\overline{\alpha_1} = \overline{f}^d(\overline{\alpha_1}) = \overline{f}^{2\cdot d}(\overline{\alpha_1}) = \dots = \overline{f}^{(n/d-1)\cdot d}(\overline{\alpha_1}),$$

and,

$$\overline{f}(\overline{\alpha_1}) = \overline{f}^{d+1}(\overline{\alpha_1}) = \overline{f}^{2\cdot d+1}(\overline{\alpha_1}) = \dots = \overline{f}^{(n/d-1)\cdot d+1}(\overline{\alpha_1})$$

and so on. □

Thus $\overline{\Phi_n}(x)$ has at least d man multiple factors each with multiplicity n/d. In fact we claim that these are the only repeated factors of $\overline{\Phi_n}(x)$. Theorem 5.1.2 shows that

$$P_c B' = \wp_1^{n/d} \dots \wp_d^{n/d} \mathfrak{q}_1 \dots \mathfrak{q}_{n(r-1)} \tag{5.8}$$

is the unique factorization of $P_c B'$ into primes of B'.

Corollary 5.2.4. *The factorization of $\overline{\Phi_n}(x)$ into monic irreducibles of $\bar{\mathbb{Q}}[x] = (B/\mathfrak{p})[x]$ has the form*

$$\overline{\Phi_n}(x) = (\overline{g_1}(x)^{n/d} \dots \overline{g_d}(x)^{n/d}) \overline{h_1}(x) \dots \overline{h_{nr-1}}(x).$$

Proof. First we claim that the hypotheses of Theorem 2.2.3 are satisfied upon substituting $(R, F, E, S, \beta, m(x), P)$ by $(A, K, K', B', \alpha, \Phi_n(x), P_c)$. That $B' = A[\alpha]$ and that $K' = K(\alpha)$ with $\alpha \in B'$ follow from 3 of Theorem 5.1.2, whereas $\Phi_n(x)$ is the minimal polynomial of α over K since it is monic, K-irreducible, and $\Phi_n(\alpha) = 0$. Therefore the hypotheses are indeed satisfied. The Corollary then follows from Theorem 2.2.3 in light of the known factorization 5.8. □

The above Corollary gives that $\overline{\Phi_n}(x)$ has d many multiple factors each with multiplicity n/d, and that these are the only multiple factors. Since we have already accounted for the d factors

$$(x - \overline{\alpha_1}), (x - \overline{f}(\overline{\alpha_1})), \dots, (x - \overline{f}^{d-1}(\overline{\alpha_1}))$$

each with multiplicity n/d, there cannot be any other multiple factors.

Theorem 5.2.5. *We have that $I_d = \langle d \cdot e_j \rangle$ for some $j \in [r]$.*

Proof. Let $\tau \in I_d$ be arbitrary. Since G acts on the zero set Z of Φ_n, and $I_d \leq G$ we must have $\tau(\alpha_1) \in Z$. Thus $\tau(\alpha_1) = f^j(\alpha_i)$ for some $i \in [r]$ and some $j \in \mathbb{Z}/n$. Now if we reduce modulo $\mathfrak{p}$, we get that

$$\overline{\alpha_1} = \overline{\tau(\alpha_1)} = \overline{f^j(\alpha_i)} = \overline{f}^j(\overline{\alpha_i}).$$

But this implies that the factor $(x - \overline{f}^j(\overline{\alpha_i}))$ of $\overline{\Phi_n}$ appears with multiplicity n/d, and we conclude that $i = 1$ so that $\tau(\alpha_1) = f^j(\alpha_1)$.

The observation

$$\overline{f^j(\alpha_1)} = \overline{\tau(\alpha_1)} = \overline{\alpha_1} = \overline{f^d(\alpha_1)} = \overline{f^{2\cdot d}(\alpha_1)} = \dots = \overline{f^{(n/d-1)\cdot d}(\alpha_1)}$$

implies that $\tau(\alpha_1) = f^j(\alpha_1) = f^{k\cdot d}(\alpha_1)$ for some $k \in \{0, \dots, \frac{n}{d} - 1\}$. But now since τ commutes with f, we get that

$$\tau(f^\ell(\alpha_1)) = f^\ell(\tau(\alpha_1)) = f^\ell(f^{k\cdot d}(\alpha_1)) = f^{k\cdot d}(f^\ell(\alpha_1))$$

for any $\ell \in \mathbb{Z}/n$. This shows that $\tau \mid_{A_1} = f^{k\cdot d} \mid_{A_1}$.

Now let $m \in \{2, \dots, r\}$ and suppose that $\tau(\alpha_m) = f^{j'}(\alpha_{i'})$ for some $i' \in [r]$ and some $j' \in \mathbb{Z}/n$, or equivalently

$$(x - \overline{\alpha_m}) = (x - \overline{f}^{j'}(\overline{\alpha_{i'}})).$$

Since $m \neq 1$, the factor $(x - \overline{\alpha_m})$ must divide $\overline{\Phi_n}$ with multiplicity 1, and then the above equality forces that $i' = m$ and $j' = 0$. Thus, $\tau(\alpha_m) = \alpha_m$ and we conclude that $\tau_{A_m} = \mathrm{Id}_{A_m}$ for every $m \in [r]$ with $m \neq 1$.

To summarize, we proved that $\tau \mid_{A_1} = f^{k \cdot d} \mid_{A_1}$ for some $k \in \{0, \ldots, \frac{n}{d} - 1\}$, whereas $\tau \mid_{A_m} = \mathrm{Id}_{A_m}$ for every $m \neq 1$. But this is precisely what it means that $\tau = (f_1^d)^k \in \langle f_1^d \rangle \equiv \langle d \cdot e_1 \rangle$ (see 4.3 to recall the definition of f_1). Thus $I_d \leq \langle d \cdot e_1 \rangle$. The equality follows from that the observation that I_d and $\langle d \cdot e_1 \rangle$ are both cyclic groups of order n/d; that this is true for I_d follows immediately from Proposition 5.2.1. □

Chapter 6

Genus Bounds for Maximal Subgroups

Here we give a description of the types of maximal subgroups which can occur inside a semi-direct product. Here is the set-up:

6.1 Flavors of Maximals

- Let G be any **finite group**.
- Let $N \trianglelefteq G$ be any **normal subgroup** of G, and further assume that N is abelian.
- Let $\Gamma := G/N$ be the **quotient group** and $\pi : G \twoheadrightarrow \Gamma$ the standard **quotient/projection map**.
- Assume that π splits. Then according to Lemma 4.1.4, G is isomorphic to the semi-direct product $N \rtimes \Gamma$, where the Γ-action on N (by automorphisms of N) is conjugation in G.
- Let $\mathrm{Max}(G)$ denote the set of all **maximal subgroups of** G, and let $M \in \mathrm{Max}(G)$ be an arbitrary maximal subgroup of G.

Lemma 6.1.1. *If $\pi(M) \lneq \Gamma$, then $N \leq M$, and $\pi(M) \in \mathrm{Max}(\Gamma)$.*

Proof. We start by observing that

$$\pi(NM) = \pi(N)\pi(M) = \pi(M) \lneq \Gamma.$$

Then this implies that $NM \lneq G$, since otherwise $\pi(NM) = \pi(G) = \Gamma$. So we see that

$$M \leq NM \lneq G.$$

As $M \in \mathrm{Max}(G)$, the only possibility is that $M = NM$. But now, if $n \in N$ then

$$n = n \cdot 1 \in NM = M$$

which proves that $N \leq M$.

By the Correspondence Theorem for Maximal Subgroups, the mapping $M \mapsto \pi(M)$ gives (one half of) an inclusion preserving bijection

$$\{M \in \mathrm{Max}(G) \mid M \leq N\} \rightleftarrows \mathrm{Max}(\Gamma).$$

This shows that $\pi(M) \in \mathrm{Max}(\Gamma)$. □

If M is a maximal subgroup of G for which $\pi(M) \lneq \Gamma$, then we say that M is a **chocolate maximal subgroup of** G. We will write $\mathrm{Max}_C(G)$ for the **set of all chocolate maximal subgroups of** G.

Let $\mathrm{Sub}(N)^\Gamma$ denote the set of all Γ**-invariant subgroups of** N:

$$\mathrm{Sub}(N)^\Gamma := \{H \leq N \mid {}^\gamma H = H, \text{ for every } \gamma \in \Gamma\}.$$

A **maximal** Γ**-invariant subgroup of** N is any maximal element of $\mathrm{Sub}(N)^\Gamma$. By this, we mean any element $H \in \mathrm{Sub}(N)^\Gamma$ such that $H \lneq N$ and which satisfies the following property: if $H' \in \mathrm{Sub}(N)^\Gamma$ satisfies that $H \leq H' \lneq N$, then $H' = H$. We will let $\mathrm{Max}(N)^\Gamma$ denote the **set of all maximal** Γ**-invariant subgroups of** N.

Lemma 6.1.2. *If $\pi(M) = \Gamma$, then $N \cap M$ is a maximal Γ-invariant subgroup of N.*

Proof. First of all, $N \cap M \in \mathrm{Sub}(N)^\Gamma$:

Let $C \in \mathrm{Sub}(N)^\Gamma$ be such that

$$N \cap M \leq C \lneq N.$$

We claim that $CM \cap N = C$.

Since $C \leq N$ and $C \leq CM$, we get $C \leq CM \cap N$. Conversely, let $a \in CM \cap N$. Then $a \in N$ and $a = cm$ for some $c \in C$ and some $m \in M$. Rearranging, we see $m = c^{-1}a$. But now $c^{-1} \in C \leq N$ and $a \in N$ imply that $m \in N$. Thus $m \in N \cap M \leq C$, so $m \in C$ and $a = cm \in C$. This proves that $CM \cap N \leq C$ and we've shown that $CM \cap N = C$.

Notice that $CM \lneq G$ since otherwise we get that

$$C = CM \cap N = G \cap N = N;$$

a contradiction. Thus we see that

$$M \leq CM \lneq G,$$

and immediately conclude that $CM = M$ since $M \in \mathrm{Max}(G)$.

Finally we are in a position to prove that $C = N \cap M$. We've already assumed that $N \cap M \leq C$, so let $c \in C$. On one hand, $c \in C \leq N$, so $c \in N$. On the other, $c \in C \leq CM = M$, so $c \in M$. Thus $c \in N \cap M$ and $C \leq N \cap M$ as a consequence. So we conclude that $C = N \cap M$ which shows that $N \cap M$ is a maximal element of $\mathrm{Sub}(N)^\Gamma$. □

If M is a maximal subgroup of G for which $\pi(M) = \Gamma$, then we say that M is a **vanilla maximal subgroup of** G. We will let $\mathrm{Max}_V(G)$ denote the **set of all vanilla maximal subgroups of** G.

6.2 Vanilla maximal subgroups

In this section, we will give genus bounds for dynatomic modular curves X_M where M is a vanilla maximal subgroup of G. We first recall a standard result from group theory which we will repeatedly use in this section. See [3, Theorem 18 of Chapter 3].

Theorem 6.2.1 ("Diamond Isomorphism Theorem")**.** *Let G be a group and let $S, N \leq G$ be subgroups with $N \trianglelefteq G$. Then $S \cap N \trianglelefteq S$ and we have $SN/N \cong S/(S \cap N)$. As a consequence we have*

$$[SN : N] = [S : S \cap N], \text{ and } [SN : S] = [N : S \cap N].$$

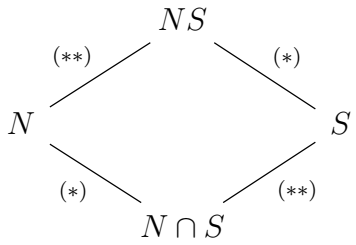


Figure 6.1: The Diamond Isomorphism Theorem.

6.2.1 Sylow theory and Γ-modules

Let Γ be any group. Recall that a **(left) Γ-module** is any abelian group A together with a left Γ-action which satisfies ${}^{\gamma}(a+b) = {}^{\gamma}a + {}^{\gamma}b$ for every $\gamma \in \Gamma$ and all $a, b \in A$. Let A be any finite Γ-module, and suppose that

$$|A| = \ell_1^{e_1} \dots \ell_s^{e_s}$$

is the prime factorization of $|A|$. Since A is abelian, every subgroup of A is normal. In particular, for each $i \in [s]$, there is a unique ℓ_i-Sylow subgroup Λ_i of A. By the prime factorization of $|A|$ we have that $|\Lambda_i| = \ell_i^{e_i}$ for each $i \in [s]$.

Lemma 6.2.2. *Λ_i is a Γ-invariant subgroup of A for every $i \in [s]$.*

Proof. Let $\gamma \in \Gamma$ and $i \in [s]$ be arbitrary. We must show that ${}^{\gamma}\Lambda_i = \Lambda_i$. Observe that it suffices to show that $|{}^{\gamma}\Lambda_i| = |\Lambda_i|$, since then ${}^{\gamma}\Lambda_i$ is a ℓ_i-Sylow subgroup of A, and by uniqueness we must have ${}^{\gamma}\Lambda_i = \Lambda_i$.

The inequality $|{}^{\gamma}\Lambda_i| \leq |\Lambda_i|$ is immediate. Now notice that ${}^{\gamma}a = {}^{\gamma}b$ for some $a, b \in \Lambda_i$ if and only if

$${}^{\gamma}a - {}^{\gamma}b = 0 = {}^{\gamma}0 \iff {}^{\gamma}(a-b) = {}^{\gamma}0 \iff a - b = 0$$

which proves that $a = b$ and therefore $|\Lambda_i| \leq |{}^{\gamma}\Lambda_i|$. □

Now let $B \leq A$ be any subgroup of A.

Lemma 6.2.3. *We have that*

$$A = \bigoplus_{k \in [s]} \Lambda_k, \text{ and } B = \bigoplus_{k \in [s]} (B \cap \Lambda_k).$$

Proof. Since A has a unique ℓ_i-Sylow subgroup for every prime ℓ_i dividing $|A|$, the first equality is a standard result. Another standard result gives that $B \cap \Lambda_k$ is the unique ℓ_k-Sylow of B for every $k \in [s]$, so we replace A by B and Λ_k by $B \cap \Lambda_k$ in the first equality in order to obtain the second equality. □

Lemma 6.2.4. *If $\Lambda_i \not\subseteq B$ and $\Lambda_j \not\subseteq B$ for $i, j \in [s]$ with $i \neq j$, then*

$$B \lneq B + \Lambda_i \lneq A.$$

Proof. First note that $B + \Lambda_i \supseteq B$. If these two sets are equal, then for every $\lambda \in \Lambda_i$ we have

$$\lambda = 0 + \lambda \in B + \Lambda_i = B \iff \Lambda_i \subseteq B,$$

so $B \lneq B + \Lambda_i$. Repeating the same argument with Λ_j in place of Λ_i shows that $B \lneq B + \Lambda_j$.

Since A is abelian, each of its subgroups is normal, and the same is true of subgroups of subgroups of A, and so on. Thus by choosing $N = B$ and $S = \Lambda_i$ in the Diamond Isomorphism Theorem 6.2.1, we get that

$$[B + \Lambda_i : \Lambda_i] = [B : B \cap \Lambda_i], \text{ and } [B + \Lambda_i : B] = [\Lambda_i : B \cap \Lambda_i].$$

Now $B \cap \Lambda_i$ is a proper subgroup of Λ_i (since otherwise $\Lambda_i \subseteq B$), and $|\Lambda_i| = \ell_i^{e_i}$, so by Lagrange's Theorem we see that $|B \cap \Lambda_i| = \ell_i^{f_i}$ for some $f_i < e_i$. Thus,

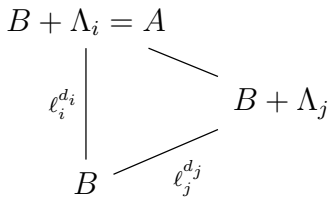
$$[B + \Lambda_i : B] = [\Lambda_i : B \cap \Lambda_i] = \ell_i^{d_i}$$

where $d_i := e_i - f_i > 0$, and a symmetric argument shows that

$$[B + \Lambda_j : B] = [\Lambda_j : B \cap \Lambda_j] = \ell_j^{d_j}$$

with $d_j := e_j - f_j > 0$.

Let us now assume (toward a contradiction) that $B + \Lambda_i = A$. Then we have a diagram



from which we deduce the contradiction that $\ell_j^{d_j}$ divides $\ell_i^{d_i}$. Therefore $B + \Lambda_i \lneq A$ and we are done. □

Proposition 6.2.5. *If $B \in \mathrm{Max}(A)$, then $[A : B] = \ell_i$ for some $i \in [s]$.*

Proof. First we claim that $B \lneq A$ implies that there is some $i \in [s]$ with $\Lambda_i \not\subseteq B$. Otherwise for every $k \in [s]$ we have $\Lambda_k \subseteq B \iff B \cap \Lambda_k = \Lambda_k$. But then

$$B = \bigoplus_{k \in [s]} (B \cap \Lambda_k) = \bigoplus_{k \in [s]} \Lambda_k = A$$

which is a contradiction. In fact i is the only $k \in [s]$ with $\Lambda_k \not\subseteq B$ since otherwise we can use Lemma 6.2.4 to see that $B \notin \mathrm{Max}(A)$.

Assume (without a loss of generality) that $i = 1$, so that $\Lambda_1 \not\subseteq B$ but $\Lambda_k \subseteq B$ for every $k \in \{2, \ldots, s\}$. First we show that $A = B + \Lambda_1$. Let $a \in A$ be arbitrary. By Lemma 6.2.3 we can write $a = \lambda_1 + \ldots + \lambda_s$ with $\lambda_k \in \Lambda_k$ for every $k \in [s]$. But then $\lambda_2, \ldots, \lambda_s \in B$ since $\Lambda_2, \ldots, \Lambda_s \subseteq B$, and therefore $a = \lambda_1 + b = b + \lambda_1 \in B + \Lambda_1$ where $b := \lambda_2 + \ldots + \lambda_s \in B$. We have established that $A \subseteq B + \Lambda_1$, and the reverse containment holds by construction.

In the proof of the previous Lemma, we showed that $[\Lambda_1 : B \cap \Lambda_1] = \ell_1^{d_1}$ for some $d_1 > 0$. Now if we choose $N = B$ and $S = \Lambda_1$ in the Diamond Isomorphism Theorem 6.2.1, we get that

$$[A : B] = [B + \Lambda_1 : B] = [\Lambda_1 : B \cap \Lambda_1] = \ell_1^{d_1}$$

with $d_1 > 0$.

Our aim is to show that $d_1 = 1$. Since $\ell_1^{d_1} = [A : B] = |A/B|$, and A/B is a group, there is some element of A/B of order ℓ_1 which generates a cyclic subgroup $\bar{C} \leq A/B$ with $\left|\bar{C}\right| = \ell_1$. Then $\bar{C}$ corresponds to a subgroup $C \leq A$ with $B \subseteq C$ under the quotient map $A \twoheadrightarrow A/B$ which sends C to $\bar{C} = C/B$. If $C = A$, then

$$\ell_1 = \left|\bar{C}\right| = |C/B| = |A/B| = \ell_1^{d_1}$$

which holds if and only if $d_1 = 1$.

If $C \lneq A$, then $B \leq C \lneq A$, and so $B = C$ by maximality of B. But then we obtain

$$\ell_1 = \left|\bar{C}\right| = |C/B| = 1,$$

which is a contradiction. Therefore the only possibility is that $C = A$ and $d_1 = 1$, as required. □

Theorem 6.2.6. *Now assume that $B \in \mathrm{Max}(A)^\Gamma$. Then we have that*

(1) There is some $i \in [s]$ for which $\Lambda_i \not\subseteq B$, but $\Lambda_j \subseteq B$ for every $j \in [s]$ different from i.

(2) We have that $\ell_i A \subseteq B$.

(3) A/B is an $\mathbb{F}_{\ell_i}$-vector space.

Proof. (1) In the proof of the previous Proposition, we saw that $B \lneq A$ implies that there is some $i \in [s]$ for which $\Lambda_i \subseteq B$. Now, $B \in \mathrm{Sub}(A)^\Gamma$ by hypothesis and $\Lambda_i \in \mathrm{Sub}(A)^\Gamma$ by Lemma 6.2.2. Thus

$$^\gamma(B + \Lambda_i) = {}^\gamma B + {}^\gamma \Lambda_i = B + \Lambda_i$$

for every $\gamma \in \Gamma$, which proves that $B + \Lambda_i \in \mathrm{Sub}(A)^\Gamma$ as well. If there is some $j \in [s]$ with $j \neq i$ and $\Lambda_j \not\subseteq B$, then Lemma 6.2.4 shows that

$$B \lneq B + \Lambda_i \lneq A$$

which contradicts our assumption that B is a *maximal* Γ-invariant subgroup of A.

(2) Since B is a proper subgroup of A, there is some $C \in \mathrm{Max}(A)$ which contains B. We have that $\Lambda_j \subseteq B \subseteq C$ for every $j \in [s]$ distinct from i, so we must also have that $\Lambda_i \not\subseteq C$ since otherwise $C = A$. Thus by Proposition 6.2.5, we have that $[C : A] = \ell_i$. Notice that this implies $\ell_i A \subseteq C$. Indeed, A/C is an abelian group of order ℓ_i so $A/C \cong \mathbb{Z}/\ell_i$, which then implies that

$$\ell_i A \subseteq \ker(A \twoheadrightarrow A/C) = C.$$

By the observation that $\ell_i A$ is Γ-invariant, we get that $\ell_i A = {}^{\gamma}(\ell_i A) \subseteq {}^{\gamma}C$ for every $\gamma \in \Gamma$. Since B is Γ-invariant by assumption, we also get $B \subseteq {}^{\gamma}C$ for every $\gamma \in \Gamma$. Consequently,

$$B,\ \ell_i A \subseteq \bigcap_{\gamma\in\Gamma} {}^{\gamma}C.$$

Now we show that $\cap_{\gamma\in\Gamma}{}^{\gamma}C$ is a proper Γ-invariant subgroup of A. For any $\gamma_0 \in \Gamma$ we have that

$${}^{\gamma_0}\left(\bigcap_{\gamma\in\Gamma} {}^{\gamma}C\right) = \bigcap_{\gamma\in\Gamma} {}^{(\gamma_0\gamma)}C = \bigcap_{\gamma\in\Gamma} {}^{\gamma}C$$

which proves Γ-invariance. If this intersection equals A, then for every $a \in A$ we have (in particular) that $a \in {}^{1}C = C$; a contradiction since $C \lneq A$. To summarize, $\cap_{\gamma\in\Gamma}{}^{\gamma}C$ is a proper Γ-invariant subgroup of A containing B (and $\ell_i A$). But since we assumed $B \in \mathrm{Max}(A)^{\Gamma}$, we are forced to conclude that

$$B = \bigcap_{\gamma\in\Gamma} {}^{\gamma}C \supseteq \ell_i A.$$

(3) Now, $\ell_i A$ is contained in the kernel B of the quotient map $A \twoheadrightarrow A/B$, so by the universal property of quotient groups, there is a unique homomorphism $\psi : A/\ell_i A \to A/B$ for which the diagram

$$\begin{array}{ccc} A & \twoheadrightarrow & A/B \\ \downarrow & \nearrow_{\psi} & \\ A/\ell_i A & & \end{array}$$

commutes. Furthermore $\psi : A/\ell_i A \twoheadrightarrow A/B$ is surjective since each of $A \twoheadrightarrow A/B$ and $A \twoheadrightarrow A/\ell_i A$ are surjective.

The Fundamental Theorem of Finite Abelian Groups shows that

$$A/\ell_i A \cong \bigoplus_{k=1}^{s_0} (\mathbb{Z}/p_k^{m_k})$$

where s_0 is some positive integer, and where p_k is prime and m_k is a positive integer for every $k \in [s_0]$. But multiplication by ℓ_i annihilates $A/\ell_i A$ so we get that $p_k^{m_k} = \ell_i$ for every $k \in [s_0]$, and hence

$$A/\ell_i A \cong \bigoplus_{k=1}^{s_0} \mathbb{Z}/\ell_i = (\mathbb{F}_{\ell_i})^{s_0},$$

so that $A/\ell_i A$ is an $\mathbb{F}_{\ell_i}$–vector space.

Finally we claim that the surjectivity of $\psi : A/\ell_i A \twoheadrightarrow A/B$ shows that A/B is also annihilated by multiplication by ℓ_i. Indeed, let $\bar{a} \in A/B$ be arbitrary. Then there is some $\bar{a}_i \in A/\ell_i A$ with $\psi(\bar{a}_i) = \bar{a}$, and

$$\ell_i \cdot \bar{a} = \ell_i \cdot \psi(\bar{a}_i) = \psi(\ell_i \cdot \bar{a}_i) = \psi(0) = 0.$$

So the same argument which showed $A/\ell_i A$ is an $\mathbb{F}_{\ell_i}$–vector space shows that A/B is an $\mathbb{F}_{\ell_i}$–vector space as well.

□

6.2.2 Computing ramification indices above $R_{n,d}$

In this subsection, we compute the ramification indices $e(Q \mid P_c)$ for $c \in R_{n,d}$ where d is any divisor of n with $d < n$, and for $Q \in \mathbb{P}_{L^M}(P_c)$ where M is any vanilla maximal subgroup of G (see Corollary 6.2.11). First we need a few general results.

For any divisor d of N and any $i \in [r]$ we have that $d \cdot e_i$ is the element of N with d in position i and 0 everywhere else. Then $\{d \cdot e_i, \ldots, d \cdot e_r\}$ is the standard basis for the subgroup $d \cdot N = \{(d \cdot a_1, \ldots, d \cdot a_r) \mid (a_1, \ldots, a_r) \in N\}$ of N.

Lemma 6.2.7. *Let d be any divisor of n. The following hold:*

(1) Γ acts transitively on $\{d \cdot e_1, \ldots, d \cdot e_r\}$ by conjugation.

(2) G acts transitively on $\{d \cdot e_1, \ldots, d \cdot e_r\}$ by conjugation. In particular we have that

$$\{{}^g(d \cdot e_i) : g \in G\} = \{{}^\gamma(d \cdot e_i) : \gamma \in \Gamma\} = \{d \cdot e_1, \ldots, d \cdot e_r\},$$

for every $i \in [r]$.

Proof. (1) In the semi-direct product, Γ acts on N by automorphisms of N. In particular, for any $\gamma \in \Gamma$ and any $i \in [r]$ we have that

$${}^\gamma(2 \cdot e_i) = {}^\gamma(e_i + e_i) = {}^\gamma e_i + {}^\gamma e_i = 2({}^\gamma e_i)$$

and continuing by induction, we see that ${}^\gamma(d \cdot e_i) = d({}^\gamma e_i)$ for any d. But now, ${}^\gamma e_i = e_{\gamma(i)}$ (see Lemma 4.2.3), so ${}^\gamma(d \cdot e_i) = d \cdot e_{\gamma(i)}$. This proves that Γ acts on $\{d \cdot e_1, \ldots, d \cdot e_r\}$ and then transitivity follows from Lemma 4.2.3.

(2) Let $g \in G = N\Gamma$. Then there are unique elements $\eta \in N$ and $\gamma \in \Gamma$ such that $g = \eta\gamma$. Thus,

$${}^g(d \cdot e_i) = {}^{\eta\gamma}(d \cdot e_i) = {}^\eta(d \cdot e_{\gamma(i)}) = (d \cdot e_{\gamma(i)})$$

where the last equality holds since $d \cdot e_{\gamma(i)} \in N$, and N is abelian. Thus the conjugation action of G on $\{d \cdot e_1, \ldots, d \cdot e_r\}$ is completely determined by the Γ action by conjugation. In particular, G is transitive on $\{d \cdot e_1, \ldots, d \cdot e_r\}$ since the same is true for Γ.

□

The next result is a generalization of an earlier result: Lemma 4.2.5 is obtained from Lemma 6.2.8 upon specifying $d = 1$.

Lemma 6.2.8. *Let d be any divisor of n, and let H be a subgroup of G for which $\pi(H) = \Gamma$. If there exist some $g \in G$ and some $i \in [r]$ for which ${}^g(d \cdot e_i) \in H$, then $d \cdot N \leq H$.*

Proof. Assume the hypotheses. H acts transitively on $\{d \cdot e_1, \ldots, d \cdot e_r\}$ since $\pi(H) = \Gamma$ and Γ is transitive on this set. Thus for every $j \in [r]$, there is some $h_j \in H$ for which

$$d \cdot e_j = {}^{h_j}\left({}^{g}(d \cdot e_i)\right).$$

This proves that $d \cdot e_j \in H$ since ${}^{g}(d \cdot e_i) \in H$ and $h_j \in H$. Thus $\{d \cdot e_1, \ldots, d \cdot e_r\} \subseteq H$ and consequently

$$d \cdot N = \langle d \cdot e_1, \ldots, d \cdot e_r \rangle \leq H.$$

□

Now let M be any vanilla maximal subgroup of G, i.e. $\pi(M) = \Gamma$. Then Lemma 6.1.2 gives that $N \cap M \in \mathrm{Max}(N)^{\Gamma}$: that is, $N \cap M$ is a maximal Γ-invariant subgroup of N. Suppose that

$$n = \ell_1^{n_1} \ldots \ell_s^{n_s}$$

is the prime factorization of n. Since $|N| = n^r$, we get that the prime factorization of $|N|$ is given by

$$|N| = \ell_1^{m_1} \ldots \ell_s^{m_s}$$

where $m_k = r \cdot n_k$ for every $k \in [s]$.

For each $j \in [s]$, let Λ_j denote the **unique ℓ_j-Sylow subgroup of** N. By Theorem 6.2.6 (1), there is some $i \in [s]$ for which $\Lambda_i \not\subseteq N \cap M$ and $\Lambda_j \subseteq N \cap M$ for every $j \in [s]$ distinct from i. After reordering the primes $\ell_1, \ldots, \ell_s$ (and reordering the $\Lambda_1, \ldots, \Lambda_s$ in a corresponding fashion), we may assume that $i = 1$. Thus

$$\Lambda_1 \not\subseteq N \cap M \text{ but } \Lambda_j \subseteq N \cap M \text{ for every } j \in \{2, \ldots, s\}. \tag{6.1}$$

Proposition 6.2.9. *There is some positive integer e for which $[G : M] = \ell_1^e$.*

Proof. As $\pi(M) = \Gamma$, we see that $G = N \rtimes M = NM$. We also have that $N \trianglelefteq G$, so we can apply the Diamond Isomorphism Theorem 6.2.1 to get that $[G : M] = [N : N \cap M]$. Theorem 6.2.6 (3) shows that $N/N \cap M$ is an $\mathbb{F}_{\ell_1}$–vector space. Therefore,

$$\ell_1^e = |N/N \cap M| = [N : N \cap M] = [G : M]$$

where $e \geq 1$ is the dimension of $N/N \cap M$ as an $\mathbb{F}_{\ell_1}$–vector space. □

For the remainder of the subsection, let d be some divisor of n such that $d < n$ and such that ℓ_1 does not divide d. Choose some $c \in R_{n,d}$ and some $\mathfrak{p} \in \mathbb{P}_L(P_c)$. We let I_d denote the **inertia subgroup**

$$I_d := I(\mathfrak{p} \mid P_c).$$

Theorem 6.2.10. *For every $g \in G$ we have that $[{}^{g}I_d : {}^{g}I_d \cap M] = \ell_1$.*

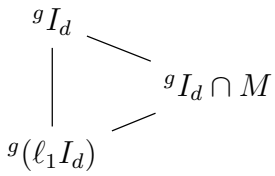
Proof. First we will show that $[{}^{g}I_d : {}^{g}I_d \cap M]$ divides ℓ_1, and then we will establish the equality by proving that $[{}^{g}I_d : {}^{g}I_d \cap M] > 1$.

Since $N \cap M$ is a maximal Γ-invariant subgroup of N, Theorem 6.2.6 (2) shows that $\ell_1 N \subseteq N \cap M$. We claim that this implies ${}^{g}(\ell_1 I_d) \subseteq {}^{g}I_d \cap M$. First of all, $\ell_1 I_d \subseteq I_d$

implies that ${}^g(\ell_1 I_d) \subseteq {}^g I_d$. Next, $I_d \subseteq N$ implies that $\ell_1 I_d \subseteq \ell_1 N$, which in turn implies ${}^g(\ell_1 I_d) \subseteq {}^g(\ell_1 N) = \ell_1 N$. Therefore

$$ {}^g(\ell_1 I_d) \subseteq \ell_1 N \subseteq N \cap M \subseteq M $$

and we have ${}^g(\ell_1 I_d) \subseteq {}^g I_d \cap M$. From the diagram



we deduce that $[{}^g I_d : {}^g I_d \cap M]$ divides $[{}^g I_d : {}^g(\ell_1 I_d)] = \ell_1$.

Having proved that $[{}^g I_d : {}^g I_d \cap M]$ divides ℓ_1, now it suffices to show that this index strictly greater than 1. First we show that $\Lambda_1 \subseteq d \cdot N$. Since N is abelian and $d \cdot N$ is a subgroup, we know that the unique ℓ_1-Sylow subgroup of $d \cdot N$ is $\Lambda_1 \cap d \cdot N$. By assumption, ℓ_1 does not divide d. Thus ℓ_1 divides $|d \cdot N|$ with multiplicity m_1 (the same multiplicity with which ℓ_1 divides $|N|$). Thus we have that $\Lambda_1 \cap d \cdot N \leq L_1$ and that $|\Lambda_1| = |\Lambda_1 \cap d \cdot N|$. The only possibility is that $\Lambda_1 = \Lambda_1 \cap d \cdot N$ which holds if and only if $\Lambda_1 \subseteq d \cdot N$.

Now we recall from Theorem 5.2.5 that $I_d = \langle d \cdot e_j \rangle$ for some $j \in [r]$. We claim that for every $g \in G$,

$$ {}^g(d \cdot e_j) \notin N \cap M $$

If there is some $g_0 \in G$ with ${}^{g_0}(d \cdot e_j) \in N \cap M \subseteq M$, then M satisfies the hypotheses of Lemma 6.2.8, and so we conclude that $d \cdot N \subseteq M$. Then this implies that $\Lambda_1 \subseteq d \cdot N \subseteq N \cap M$, which contradicts 6.1. So indeed, ${}^g(d \cdot e_j) \notin N \cap M$ for every $g \in G$.

From here we deduce that for every $g \in G$ we have ${}^g I_d \not\subseteq M$. For if there is some $g_0 \in G$ with ${}^{g_0} I_d \subseteq M$, then in particular this implies ${}^{g_0}(d \cdot e_j) \in M$. At the same time, in Lemma 6.2.7, we saw that G acts on $\{d \cdot e_1, \ldots, d \cdot e_r\}$, so that ${}^{g_0}(d \cdot e_j) = d \cdot e_k \in N$ for some $k \in [r]$. Thus if ${}^{g_0} I_d \subseteq M$, then ${}^{g_0}(d \cdot e_j) \in N \cap M$. But we showed this cannot happen in the previous paragraph. Thus for every $g \in G$, we have

$$ {}^g I_d \not\subseteq M \iff {}^g I_d \cap M \subsetneq {}^g I_d \iff [{}^g I_d : {}^g I_d \cap M] > 1, $$

and we are done. □

Corollary 6.2.11. *Recall that d is any divisor of n such that $d < n$ and ℓ_1 does not divide d. For every $c \in R_{n,d}$ and every $Q \in \mathbb{P}_{L^M}(P_c)$ we have that the ramification index $e(Q \mid P_c)$ equals ℓ_1.*

Proof. According to Corollary 2.2.15, we have that

$$ \{e(Q \mid P_c) : Q \in \mathbb{P}_{L^M}(P_c)\} = \{[{}^g I_d : {}^g I_d \cap M] : g \in G\}. $$

We are done by Theorem 6.2.10 since $[{}^g I_d : {}^g I_d \cap M] = \ell_1$ for every $g \in G$. □

6.2.3 Lower bounds on $g(X_M)$ for vanilla maximals M

Recall that $K = \bar{\mathbb{Q}}(t)$, that L is the splitting field over K of $\Phi_n(x)$, that K' denotes the primitive K-extension $\frac{K[x]}{(\Phi_n(x))}$, and that $\mathbb{P}$ denotes the set of all places of K which ramify in K'. Recall also that Morton showed $\mathbb{P} = \{P_\infty\} \sqcup \{P_c : c \in \sqcup_{d|n} R_{n,d}\}$ (see Theorem 5.1.2).

Let M be any vanilla maximal subgroup of G, and suppose that ℓ is the unique prime dividing n for which $\Lambda \not\subseteq N \cap M$, where Λ is the unique ℓ-Sylow subgroup of N. Then by Proposition 6.2.9, we have that $[G : M] = \ell^e$ for some positive integer e. Then the Riemann-Hurwitz genus formula 3.2.4 gives that

$$\begin{aligned} 2g(L^M) - 2 &= (-2)[G : M] + \sum_{P \in \mathbb{P}} \sum_{Q \in \mathbb{P}_{L^M}(P)} (e(Q \mid P)) \\ &= -2\ell^e + \gamma_\infty + \sum_{d|n} \gamma_d \end{aligned}$$

where

$$\gamma_\infty := \sum_{Q \in \mathbb{P}_{L^M}(P_\infty)} (e(Q \mid P_\infty) - 1)$$

and where

$$\gamma_d := \sum_{c \in R_{n,d}} \sum_{Q \in \mathbb{P}_{L^M}(P_c)} (e(Q \mid P_c) - 1)$$

for every d dividing n. Solving for $g(L^M)$, we get that

$$g(L^M) = 1 - \ell^e + \frac{1}{2}\left(\gamma_\infty + \sum_{d|n} \gamma_d\right) = 1 - \ell^e + \frac{\gamma_1}{2} + \frac{\gamma^*}{2} \tag{6.2}$$

where

$$\gamma_* := \gamma_\infty + \sum_{\substack{d|n, \\ d>1}} \gamma_d \geq 0.$$

Now we focus our attention on the contribution to 6.2 coming from γ_1:

$$\gamma_1 = \sum_{c \in R_{n,1}} \sum_{Q \in \mathbb{P}_{L^M}(P_c)} (e(Q \mid P_c) - 1).$$

For every $n \geq 2$, the divisor $d = 1$ of n satisfies that $d < n$ and ℓ does not divide d. Thus Corollary 6.2.11 gives that $e(Q \mid P_c) = \ell$ for every $c \in R_{n,1}$ and every $Q \in \mathbb{P}_{L^M}(P_c)$, and we conclude that

$$\begin{aligned} \gamma_1 &= \sum_{c \in R_{n,1}} \sum_{Q \in \mathbb{P}_{L^M}(P_c)} (\ell - 1) \\ &= \sum_{c \in R_{n,1}} |\mathbb{P}_{L^M}(P_c)| \, (\ell - 1). \end{aligned}$$

By Proposition 2.2.2 we have that

$$\ell^e = [G : M] = [L^M : K] = \sum_{Q \in \mathbb{P}_{L^M}(P_c)} e(Q \mid P_c) f(Q \mid P_c) = |\mathbb{P}_{L^M}(P_c)|\, \ell. \tag{6.3}$$

(We are using that $f(Q \mid P_c) = 1$ for every Q since our residue field at the bottom is $\bar{\mathbb{Q}}$). As a consequence,

$$\begin{aligned}
\gamma_1 &= \sum_{c \in R_{n,1}} |\mathbb{P}_{L^M}(P_c)|\,(\ell - 1) \\
&= \sum_{c \in R_{n,1}} \ell^{e-1}(\ell - 1) \\
&= |R_{n,1}|\,(\ell^e - \ell^{e-1}) \\
&= \varphi(n)(\ell^e - \ell^{e-1})
\end{aligned}$$

where φ is Euler's φ-function—see Theorem 5.1.1. We have proved the following:

Proposition 6.2.12. *Let M be a vanilla maximal subgroup of G, and let ℓ and e denote the prime and positive integer for which $[G : M] = \ell^e$. Then we have that*

$$\begin{aligned}
g(L^M) &= 1 - \ell^e + \frac{1}{2}\gamma_1 + \frac{1}{2}\gamma^* \\
&\geq 1 - \ell^e + \frac{1}{2}\gamma_1 \\
&= 1 - \ell^e + \frac{\varphi(n)}{2}(\ell^e - \ell^{e-1})
\end{aligned}$$

Corollary 6.2.13. *For $n = 11$ and for every $n \geq 13$ the following holds: for every vanilla maximal subgroup M of the n-th dynatomic Galois group G, we have $g(L^M) \geq 2$.*

Proof. First, for $n = 11$ and for every $n \geq 13$, we have $\varphi(n) \geq 6$. Indeed, for $n = 11$ and for every integer n in the range $[13, 71]$ we verify by direct computation that $\varphi(n) \geq 6$ (see Table 6.1), and for $n \geq 72$ we can use the well known lower bound $\varphi(n) \geq \sqrt{n/2}$ (see for example [14, Proposition 2]).

Thus for $n = 11$ and $n \geq 13$ we have

$$g(L^M) \geq 1 - \ell^e + 3(\ell^e - \ell^{e-1}) = 1 + 2\ell^e - 3\ell^{e-1} = 1 + \ell^{e-1}(2\ell - 3)$$

according to Proposition 6.2.12. But now even in the worst possible case where $e = 1$, the quantity $1 + \ell^{e-1}(2\ell - 3)$ is at least 2 for every prime ℓ. □

Having proved the above Corollary, we now know that for $n \in \{5, 6, 7, 9, 11\}$, and every $n \geq 13$, we have $g(X_M) \geq 2$ for every vanilla maximal subgroup M of G. (In [8], Krumm showed that for $n \in \{5, 6, 7, 9\}$ the bound $g(X_M) \geq 2$ holds for *every* maximal subgroup M,

$\mathbf{n}$	$\varphi(\mathbf{n})$	$\mathbf{n}$	$\varphi(\mathbf{n})$	$\mathbf{n}$	$\varphi(\mathbf{n})$	$\mathbf{n}$	$\varphi(\mathbf{n})$
10	4	27	18	44	20	61	60
11	10	28	12	45	24	62	30
12	4	29	28	46	22	63	36
13	12	30	8	47	46	64	32
14	6	31	30	48	16	65	48
15	8	32	16	49	42	66	20
16	8	33	20	50	20	67	66
17	16	34	16	51	32	68	32
18	6	35	24	52	24	69	44
19	18	36	12	53	52	70	24
20	8	37	36	54	18	71	70
21	12	38	18	55	40	72	24
22	10	39	24	56	24	73	72
23	22	40	16	57	36	74	36
24	8	41	40	58	28	75	40
25	20	42	12	59	58	76	36
26	12	43	42	60	16	77	60

Table 6.1: The values n and $\varphi(n) = |R_{n,1}|$ for $10 \leq n \leq 77$.

so in particular it holds for the vanilla maximals M). It is natural to ask then *"what about $n = 8, 10, 12$?"*

In the previous corollary, we were able to prove that $g(X_M) \geq 2$ by only considering contributions to the Riemann-Hurwitz formula coming from $R_{n,1}$. For each of $n = 8, 10, 12$, we have that $\varphi(n) = 4$, and we cannot rule out the possibility that the prime ℓ is 2 (remember that ℓ must divide n). While it is still true for $n = 8, 10, 12$ that

$$g(L^M) \geq 1 - \ell^e + \frac{1}{2}\gamma_1 = 1 - \ell^e + \frac{\varphi(n)}{2}(\ell^e - \ell^{e-1}),$$

if we plug in $\ell = 2$ and $\varphi(n) = 4$ we get that

$$1 - \ell^e + \frac{1}{2}\gamma_1 = 1 - 2^e + 2(2^e - 2^{e-1}) = 1 \tag{6.4}$$

for every $e > 0$, and all we can say using this method is that $g(L^M) \geq 1$. Thus if we are to have any hope at proving $g(L^M) \geq 2$ for every vanilla M and $n \in \{8, 10, 12\}$, we will need to consider contributions to genus coming from the term

$$\gamma_* = \gamma_\infty + \sum_{\substack{d|n,\\ d>1}} \gamma_d.$$

Theorem 6.2.14. *Let $n \in \{10, 12\}$. Then for every vanilla maximal subgroup M of G, we have that $g(L^M) \geq 2$.*

Proof. Assume first that $n = 10$. Then $\ell \in \{2, 5\}$ and $\varphi(n) = 4$.

If $\ell = 5$, then

$$g(L^M) \geq 1 - \ell^e + \frac{\varphi(n)}{2}(\ell^e - \ell^{e-1}) = 1 - 5^e + 2(5^e - 5^{e-1}).$$

Even if we assume the worst possible case of $e = 1$, we get that

$$g(L^M) \geq 1 - 5 + 2(5 - 1) = 4 \geq 2.$$

Now suppose that $n = 10$ and $\ell = 2$. We consider the divisor $d = 5$ of 10. Since $\ell = 2$ does not divide $d = 5$, Corollary 6.2.11 gives that $e(Q \mid P_c) = 2$ for every $c \in R_{10,5}$ and every $Q \in \mathbb{P}_{L^M}(P_c)$. Thus,

$$\gamma_5 = \sum_{c \in R_{10,5}} |\mathbb{P}_{L^M}(P_c)|(2 - 1).$$

By the same argument from 6.3, we have that $|\mathbb{P}_{L^M}(P_c)| = \ell^{e-1} = 2^{e-1}$ for any $c \in R_{10,5}$. Thus after computing (using Theorem 5.1.1) that $|R_{10,5}| = 15$, we find that

$$\gamma_5 = |R_{10,5}| \cdot 2^{e-1}(2 - 1) = 15 \cdot 2^{e-1}$$

for every $e > 0$. Combining the above with 6.4, we obtain

$$\begin{aligned} g(L^M) &= 1 - 2^e + \frac{1}{2}(\gamma_\infty + \gamma_1 + \gamma_2 + \gamma_5 + \gamma_{10}) \\ &\geq 1 - 2^e + \frac{1}{2}\gamma_1 + \frac{1}{2}\gamma_5 \\ &= 1 + \frac{1}{2}\gamma_5 \\ &= 1 + \frac{1}{2}(15 \cdot 2^{e-1}) > 2. \end{aligned}$$

Now assume that $n = 12$. Then $\ell \in \{2, 3\}$ and $\varphi(n) = 4$.

If $\ell = 3$, then

$$g(L^M) \geq 1 - \ell^e + \frac{\varphi(n)}{2}(\ell^e - \ell^{e-1}) = 1 - 3^e + 2(3^e - 3^{e-1}).$$

Even if the worst possible case of $e = 1$ holds, then the above equals $1 - 3 + 2(3 - 1) = 2$ and we still get $g(L^M) \geq 2$.

If $n = 12$ and $\ell = 2$, then we choose the divisor $d = 3$ of n and again by Corollary 6.2.11, we see that $e(Q \mid P_c) = 2$ for every $c \in R_{12,3}$ and every $Q \in \mathbb{P}_{L^M}(P_c)$. By the same argument given for $n = 10$, and $d = 5$ we get that

$$\gamma_3 = |R_{12,3}| \cdot 2^{e-1}(2 - 1) = 6 \cdot 2^{e-1}$$

(Here again we computed $|R_{12,3}| = 6$ using Theorem 5.1.1). Riemann-Hurwitz gives that

$$\begin{aligned} g(L^M) &= 1 - 2^e + \frac{1}{2}(\gamma_\infty + \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 + \gamma_6 + \gamma_{12}) \\ &\geq 1 - 2^e + \frac{1}{2}\gamma_1 + \frac{1}{2}\gamma_3 \\ &= 1 + \frac{1}{2}(6 \cdot 2^{e-1}) > 2. \end{aligned}$$

□

Now we can combine Corollary 6.3.4 with Theorem 6.2.14 to obtain the following:

Corollary 6.2.15. *For every $n \geq 10$ and every Vanilla maximal subgroup M of G, we have that $g(X_M) \geq 2$.*

Thus we have handled the cases $n = 10$ and $n = 12$ using only a slight modification of the methods which worked for $n = 11$ and $n \geq 13$. Again though, $n = 8$ is conspicuously missing. As far as our methods so far are concerned, the problem with $n = 8$ is that there is no divisor $d > 1$ of $n = 8$ such that $\ell = 2$ does not divide d. Thus we cannot use Corollary 6.2.11 to compute ramification indices. It may even be the case that all of the primes P_c for $c \in R_{8,2} \cup R_{8,4}$ are unramified! If this holds then the only ramified places are P_∞ or those coming from $R_{8,1}$ and $R_{8,8}$. Unfortunately, we already saw that considering ramification above $R_{8,1}$ does not suffice for our goal, and understanding inertia (and ultimately ramification indices) above P_∞ and above $R_{8,8}$ seems to be more complicated.

6.3 Chocolate maximal subgroups

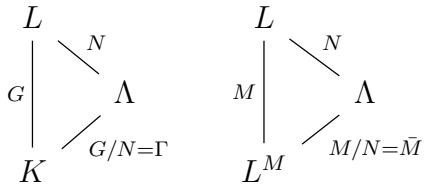
In this section we will give genus bounds for dynatomic modular curves X_M where M is a chocolate maximal subgroup of G.

6.3.1 A first reduction

First we give a reduction which allows us to consider maximal subgroups of Γ. Let M be any chocolate maximal subgroup of G, i.e., $\pi(M) \lneq \Gamma$. Then Lemma 6.1.1 shows that $N \subseteq M$ and that $\bar{M} := \pi(M) \in \mathrm{Max}(\Gamma)$.

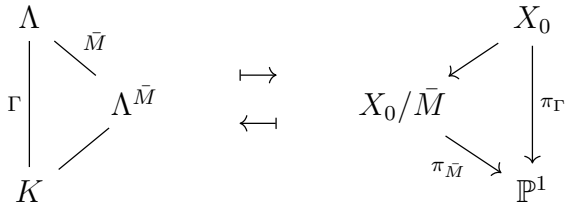
A first easy observation is that in fact $N \trianglelefteq M$. Indeed, $N \subseteq M$ implies that $N = N \cap M$. But $N \cap M$ is normal in M. Indeed, any group M is invariant under M-conjugation, and since $N \trianglelefteq G$ we have that N is invariant under H-conjugation for any subgroup $H \leq G$ (in particular for $H = M$).

Now N is normal in G with $G/N = \Gamma$. At the same time, $N \trianglelefteq M$ shows that $L^N \supseteq L^M$ and that L^N/L^M is Galois with group $M/N = \pi(M) = \bar{M}$. For the remainder of this section, we will let Λ denote L^N. Thus we get diagrams



of field extensions and Galois groups. By the Galois correspondence, $\mathrm{Gal}(\Lambda/L^M) = \bar{M}$ which holds if and only if $L^M = \Lambda^{\bar{M}}$.

Let X denote the curve in $\mathcal{C}_{\bar{\mathbb{Q}}}$ corresponding to L. We will henceforth write X_0 for the **quotient curve** X/N whose function field over $\bar{\mathbb{Q}}$ is Λ. Thus we have equivalent diagrams of function fields and curves



over $\bar{\mathbb{Q}}$. In particular notice that $\bar{\mathbb{Q}}\left(X_0/\bar{M}\right) = \Lambda^{\bar{M}}$. On the other hand, if X_M denotes the quotient curve X/M, then we get that $\bar{\mathbb{Q}}(X_M) = L^M = \Lambda^{\bar{M}} = \bar{\mathbb{Q}}\left(X_0/\bar{M}\right)$. We have proved the following:

Lemma 6.3.1. *We have that* $g(X_M) = g\left(X_0/\bar{M}\right)$.

We have therefore reduced our task to giving genus bounds for curves $X_0/\bar{M}$ for maximal subgroups $\bar{M}$ of Γ.

6.3.2 A theorem of Guralnick and Shareshian

Recall that $K = \bar{\mathbb{Q}}(t)$. Let Λ/K be any extension of function fields over $\bar{\mathbb{Q}}$ and let $\Gamma := \mathrm{Gal}(\Lambda/K)$. For a subgroup $H \leq \Gamma$, we will let Λ^H denote the fixed field of H in Λ.

Let X_0 denote the curve over $\bar{\mathbb{Q}}$ corresponding to Λ. Then the quotient curve X_0/H is the curve corresponding to Λ^H. We will let g_H denote the genus $g(X_0/H)$. Define

$$s := \left|\{P \in \mathbb{P}_K : P \text{ ramifies in } \Lambda\}\right|.$$

By Riemann's Existence Theorem, there exist elements $x_1, \ldots, x_s \in \Gamma$ which generate Γ and whose product equals 1 (see [6, pp. 1]).

Theorem 6.3.2 ([6, Theorem 1.1.2])**.** *Let* $\Gamma \in \{S_r, A_r\}$ *with* $r \geq 5$. *Let* $E = (x_1, \ldots, x_s)$ *be an* s*-tuple of non-identity elements of* Γ *such that* $\Gamma = \langle E \rangle$ *and such that* $\prod_{i=1}^{s} x_i = 1$. *Let* $H \neq A_r$ *be a maximal subgroup of* Γ. *Assume* $s \geq 5$. *Then there is a constant* $c \geq 0$ *which is independent of* Γ, H, *and* r, *such that one of the following conditions holds:*

(1) H *is the stabilizer of a point in the natural action of* Γ.

(2) We have

$$g_H > \max\{cr, 2\}.$$

(3) $\Gamma = S_r$*, H is the stabilizer of a 2-set in the natural action of* Γ*,* $g_H = 0$*,* $s = 5$ *and one of the following conditions holds:*

  (a) the five elements of E have cycle shapes $1^{m-2}2^1$, $1^3 2^{\frac{m-3}{2}}$, $1^1 2^{\frac{m-1}{2}}$, $1^1 2^{\frac{m-1}{2}}$, $1^1 2^{\frac{m-1}{2}}$*;*

  (b) the five elements of E have cycle shapes $1^{m-2}2^1$, $1^2 2^{\frac{m-2}{2}}$, $1^2 2^{\frac{m-2}{2}}$, $1^2 2^{\frac{m-2}{2}}$, $2^{\frac{m}{2}}$*.*

(4) One of the cases in the following conditions holds:

  (a) We have $s > 5$, $r \in \{5, 6\}$, and (Γ, H, E) is one of the finitely many triples described in [6, Theorem A.2.1];

  (b) We have $7 \leq r \leq 20$ and (Γ, H, E) is one of the finitely many triples described in [6, Theorems A.3.1 and A.3.2]

6.3.3 The number of ramified points of $X_0 \to \mathbb{P}^1$

Proposition 6.3.3. *For every $n \geq 2$ and every $c \in R_{n,n}$, the place P_c of $K/\bar{\mathbb{Q}}$ ramifies in Λ.*

Proof. Recall from Corollary 1.3.4 that we have a decomposition of the zero set

$$Z = \{\alpha \in L : \Phi_n(\alpha) = 0\} = \bigsqcup_{i=1}^{r} A_i$$

where A_i is the f-orbit $\{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ for some $\alpha_i \in L$. Define $K_i := K(\alpha_i)$, and let F_i be the fixed field in K_i of the automorphism

$$(\alpha_i \mapsto f(\alpha_i)) \in \mathrm{Aut}(K_i).$$

In [12], Morton and Patel showed that the fields $F_1, \ldots, F_r$ are all conjugates in K and that Λ is the compositum $\Lambda = F_1 \ldots F_r$. In [10], Morton showed that for every $c \in R_{n,n}$ and every $i \in [r]$

$$P_c R_{F_i} = \wp_1^2 \wp_2 \ldots \wp_k$$

is the factorization of $P_c R_{F_i}$ into primes of R_{F_i}, where R_{F_i} denotes the integral closure of $\bar{\mathbb{Q}}[t]$ in F_i. Thus P_c ramifies in each F_i, and in particular, it must ramify in $\Lambda = F_1 \ldots F_r$. □

Corollary 6.3.4. *Let*

$$s := |\{P \in \mathbb{P}_K : P \text{ ramifies in } \Lambda\}|.$$

Then for every $n \geq 5$, we have $s \geq 11$.

Proof. The previous Proposition shows that $s \geq |R_{n,n}|$. But for every $n \geq 5$, we have that $|R_{n,n}| \geq 11$. Indeed, $|R_{5,5}| = 11$, and $|R_{n,n}|$ grows exponentially with n (see Table 6.2). □

Theorem 6.3.5. *For every $n \geq 5$ and every chocolate maximal subgroup M of the n-th dynatomic Galois group G, we have $g(X_M) \geq 2$.*

$\mathbf{n}$	$\lvert\mathbf{R_{n,n}}\rvert$	$\mathbf{n}$	$\lvert\mathbf{R_{n,n}}\rvert$
2	0	11	1013
3	1	12	1959
4	3	13	4083
5	11	14	8052
6	20	15	16315
7	57	16	32496
8	108	17	65519
9	240	18	130464
10	472	19	262125

Table 6.2: $|R_{n,n}|$ grows very rapidly with n.

Proof. In [8], Krumm showed that for $n \in \{5, 6, 7, 9\}$, the genus $g(X_M) \geq 2$ for *every* maximal subgroup M of G, so in particular $g(X_M) \geq 2$ for every chocolate maximal for these values of n.

So assume $n \geq 8$. Recall that $r = \frac{\deg \Phi_n(x)}{n}$, and that r is also the number of f-orbits forming the decomposition of the zero set of Φ_n appearing in Corollary 1.3.4. Now we will apply Theorem 6.3.2 to the particular case $\Gamma = G/N = S_r$ and $H = \bar{M}$, where M is any chocolate maximal subgroup of G. By Riemann's Existence Theorem, we can take s to be the number of points of K which ramify in $\Lambda = L^N$ (see the paragraph preceding Theorem 6.3.2). For $n \geq 8$, we have $r \geq 30$ (see Table 6.3) so we can eliminate the possibility that (4) in Theorem 6.3.2 holds. Furthermore, $n \geq 8$ implies $s > 5$, so (3) of Theorem 6.3.2 cannot hold either. Finally, if we are in case (1) of Theorem 6.3.2, then we can use [10, Theorem C] to prove that $g(X_0/\bar{M}) \geq 2$ for every $n \geq 8$ and every maximal subgroup $\bar{M}$ of $\Gamma = S_r$. So case (1) or case (2) of Theorem 6.3.2 must hold, and in either case we have that for every chocolate maximal subgroup M of G, the genus $g(X_0/\bar{M}) \geq 2$.

Thus, according to Lemma 6.3.1, we get that for every $n \geq 5$ and every chocolate maximal subgroup M of G we have $g(X_M) = g(X_0/\bar{M}) \geq 2$. □

n	r	n	r
2	1	11	186
3	2	12	335
4	3	13	630
5	6	14	1161
6	9	15	2182
7	18	16	4080
8	30	17	7710
9	56	18	14532
10	99	19	27594

Table 6.3: The values n and $r = \frac{\deg \Phi_n}{n}$ for $2 \leq n \leq 19$.

Chapter 7

Finitely many exceptional values

We are finally equipped to prove the main result of the thesis.

Theorem 7.0.1. *For every $n \geq 10$ there are at most finitely many values $c \in \mathbb{Q}$ such that $f_c(x) = x^2 + c$ has a point of period n in $\mathbb{Q}$.*

Proof. We proved that for these n values, $g(X_M) \geq 2$ for every vanilla maximal subgroup M of G (Corollary 6.2.15) and we proved that the same is true for every chocolate maximal subgroup M of G (Theorem 6.3.5). Thus, since an arbitrary maximal subgroup M of G must be chocolate or vanilla (depending on whether $\pi(M)$ is all of Γ), we have proved that for every $n \geq 10$ we have $g(X_M) \geq 2$ for *every* maximal subgroup of G. Therefore, by Proposition 3.2.6 the exceptional set E_n is finite for these values of n. But then by Theorem 2.3.8, there are at most finitely many values $c \in \mathbb{Q}$ such that the set $\mathrm{Per}_n(f_c; \mathbb{Q})$ (of all n-periodic points of f_c in $\mathbb{Q}$) is non-empty. □

Bibliography

[1] Robert Benedetto, Patrick Ingram, Rafe Jones, Michelle Manes, Joseph H. Silverman, and Thomas J. Tucker. Current trends and open problems in arithmetic dynamics. *Bull. Amer. Math. Soc. (N.S.)*, 56(4):611–685, 2019.

[2] Thierry Bousch. *Sur quelques problemes de dynamique holomorphe*. PhD thesis, Paris 11, 1992.

[3] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, second edition, 1999.

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

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

[6] Robert M. Guralnick and John Shareshian. Symmetric and alternating groups as monodromy groups of Riemann surfaces. I. Generic covers and covers with many branch points. *Mem. Amer. Math. Soc.*, 189(886):vi+128, 2007. With an appendix by Guralnick and R. Stafford.

[7] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[8] David Krumm. A finiteness theorem for specializations of dynatomic polynomials. *Algebra & Number Theory*, 13(4):963–993, 2019.

[9] David Krumm and Nicole Sutherland. Galois groups over rational function fields and explicit Hilbert irreducibility. *J. Symbolic Comput.*, 103:108–126, 2021.

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

[11] Patrick Morton. Arithmetic properties of periodic points of quadratic maps, ii. *Acta Arithmetica*, 87(2):89–102, 1998.

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

[13] Patrick Morton and Franco Vivaldi. Bifurcations and discriminants for polynomial maps. *Nonlinearity*, 8(4):571–584, 1995.

[14] Francois Nicolas. A simple, polynomial-time algorithm for the matrix torsion problem, 2009.

[15] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.

[16] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[17] Michael Stoll. Rational 6-cycles under iteration of quadratic polynomials. *LMS Journal of Computation and Mathematics*, 11:367–380, 2008.

[18] Andrew Sutherland. MIT Mathematics 18.782, Lecture Notes: Arithmetic Geometry, 2013. URL: https://math.mit.edu/classes/18.782/lectures.html. Last visited on 2021/06/24.

[19] Andrew Sutherland. MIT Mathematics 18.785, Lecture Notes: Algebraic Number Theory, 2019. URL: https://ocw.mit.edu/courses/mathematics/18-785-number-theory-i-fall-2019/lecture-notes/. Last visited on 2021/06/24.