A TARGETED MARTINET SEARCH

by

Eric D. Driver

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

ARIZONA STATE UNIVERSITY

December 2006

A TARGETED MARTINET SEARCH

by

Eric D. Driver

has been approved
November 2006

APPROVED:

______________________________, Chair

Supervisory Committee

ACCEPTED:

Department Chair

Dean, Division of Graduate Studies

ABSTRACT

Constructing number fields with prescribed ramification is an important problem in computational number theory. In this dissertation, I consider the problem of generating number fields of a fixed degree which are unramified outside a given set of primes. Current methods for generating such fields use a method called the targeted Hunter search, but this method is only guaranteed to find the primitive fields. Another search technique, called the Martinet search, is used to find imprimitive fields. The standard Martinet search is designed to find all fields with a given discriminant bound and is not efficient at targeting fields with prescribed ramification. In this dissertation, the targeted search technique and the Martinet search technique are combined to form a new algorithm, called the targeted Martinet search. The targeted Martinet search is guaranteed to find all the imprimitive fields having a prescribed ramification. This new algorithm is then used to generate complete tables of imprimitive number fields for degrees 4 through 10.

For my wife, Valerie.

ACKNOWLEDGMENTS

I would like to thank my advisor, John Jones, for introducing me to this line of research, and also for his guidance along the way, especially showing me the idea behind the first proof to Theorem 3.5. I would also like to thank my employer, Lockheed Martin, for the financial assistance and for allowing me a flexible work schedule. Finally, I owe a debt of gratitude to my wife, Valerie, for all her patience and understanding throughout this fun but arduous process.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

An important problem in the study of fields is to find all number fields of a fixed degree with a given discriminant bound. A related problem, which is equally important, is to find all number fields with a prescribed ramification structure. This dissertation will focus on this second problem, and will concentrate primarily on finding all imprimitive number fields unramified outside of a finite set of primes.

One of the key theorems, which is used extensively in this line of research, is Hunter's theorem. Hunter's theorem is used to give bounds on the integer coefficients of a defining polynomial for the field. One then finds all fields by doing a computer search over all polynomials satisfying the bounds. The problem with Hunter's theorem is that it is only guaranteed to find the primitive fields (*i.e.* those with no intermediate subfields). This issue is resolved by using a relative version of Hunter's theorem, called Martinet's theorem.

For fields of degree four or higher, the standard computer searches can become computationally burdensome. We fix this by using what is called a targeted Hunter search. When the field is unramified outside a given finite set of primes, the coefficients of a defining polynomial obey certain congruence relations. By exploiting these congruences, we can reduce the number of polynomials that need checking by several orders of magnitude.

Martinet searches have been performed by Diaz Y Diaz and Olivier [4]. The targeted Hunter search has been used before for sextic and septic fields by Jones and Roberts [7, 8]. The goal of my research was to combine these two methods into what we call a targeted Martinet search, and then apply the new method to several applications.

In this chapter, I give a brief overview of the three main search techniques: the Hunter search, the Martinet search, and the targeted Hunter search. I end the chapter with a short discussion of the targeted Martinet search.

1.1. Hunter Searches

Suppose one wished to determine all algebraic number fields K of degree n with discriminant bounded by M. The primary tool used to accomplish this is Hunter's theorem:

Theorem 1.1 (Hunter). *Let K be a number field of degree n over $\mathbb{Q}$. There exists $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ such that*

$$\sum_{i=1}^{n} |\alpha_i|^2 \leq \frac{1}{n} \operatorname{Tr}(\alpha)^2 + \gamma_{n-1} \left(\frac{|d_K|}{n} \right)^{1/(n-1)},$$

where the α_i's are the conjugates of α, d_K is the discriminant of K, γ_{n-1} is Hermite's constant in dimension $n-1$, and $\mathrm{Tr}(\alpha) = \sum_{i=1}^{n} \alpha_i$ is the trace of α over $\mathbb{Q}$. Furthermore, we may assume that $0 \leq \mathrm{Tr}(\alpha) \leq \frac{n}{2}$.

Let us assume that the element α given by Hunter's theorem is primitive (which is always the case when n is prime). Let f_α be the minimal polynomial for α over $\mathbb{Q}$ and write

$$f_\alpha(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n.$$

Since $\alpha \in \mathcal{O}_K$ we must have $a_i \in \mathbb{Z}$ for each i. Hunter's theorem also tells us that $|a_1| = |\mathrm{Tr}(\alpha)| \leq \frac{n}{2}$. We can obtain bounds on the other coefficients as follows. Since d_K is bounded, so is $T_2(\alpha) \stackrel{\text{def}}{=} \sum_{i=1}^{n} |\alpha_i|^2$. Say $T_2(\alpha) \leq B$. Then for each i, $|\alpha_i| \leq \sqrt{B}$. Finally, since the a_i's are symmetric polynomials in the α_i's, one can easily obtain the following bound:

$$|a_k| \leq \binom{n}{k} B^{k/2} \qquad (k = 2, 3, \ldots, n).$$

So every primitive field K of degree n with bounded discriminant is defined by a polynomial f_α with coefficients bounded as above. The number of such polynomials is finite, hence the number of fields K is finite and these fields can be obtained by checking each candidate f_α. We reiterate that this method is only guaranteed to find all the primitive fields; a method for obtaining the imprimitive fields uses Martinet's theorem, which is discussed later.

The bounds on the a_i's computed above are actually quite weak, and there are several ways to improve these bounds. See Cohen [3](pp.445-460) for a good summary of the various methods for tightening these bounds.

The general algorithm for finding the primitive fields K of degree n with $d_K \leq M$ proceeds as follows. One starts with a set of nested loops over the a_i's. For each combination of a_i's, one forms the polynomial f_α. For f_α to be valid it must satisfy the following conditions:

1. f_α must be irreducible,
2. $T_2(\alpha)$ must satisfy Hunter's bound, and
3. $|d_K|$ must be less than or equal to M.

If all these conditions are met, then f_α is added to a list. Since some of these polynomials may generate the same field, a final step in the algorithm is to remove any duplicates from the list. An efficient method for removing duplicates is the polredabs algorithm as described in [2] (pp.170-173, algorithm 4.4.12). Polredabs transforms each polynomial into a new polynomial which defines the same field but has a simplified pseudo-canonical form. Two polynomials which define the same field will most likely be reduced to the same form by polredabs, allowing the easy removal of almost all the duplicates. To weed out the last remaining duplicates, we use the nfisisom subroutine from the pari-gp library [2] (pp.179-180).

Now suppose one wanted to determine all fields K of degree n which were unramified outside a finite set of primes S. Such a field K would have discriminant of the form

$$d_K = \pm \prod_{p_i \in S} p_i^{r_i}.$$

A famous result from algebraic number theory tells us that the exponents r_i are finite. In fact, one can show the following result which gives a maximum bound for the discriminant:

Theorem 1.2. *Let K be a number field of degree n over $\mathbb{Q}$. Let p be a prime at which K is ramified. Write n as $n = a_r p^r + \cdots + a_1 p + a_0$ where $0 \le a_i \le p-1$ and let $T = \{\ i \mid a_i \neq 0\}$. Then the upper bound for the exponent of p in d_K is*

$$B = n - |T| + \sum_{i \in T} i a_i p^i.$$

Now that we have an upper bound on $|d_K|$, we may apply our earlier results to find all the primitive fields K of degree n which are unramified outside of S. Although easy to implement, this approach is also very inefficient. We will see in section 1.3 how the ramification structure of p can be used to obtain congruences on the coefficients of f_α, thereby improving computation time by orders of magnitude.

1.2. Martinet Searches

In the previous section, we showed how Hunter's theorem could be used to find number fields K with bounded discriminant. Hunter's theorem is only guaranteed to find all the primitive fields. In order to find the imprimitive fields, one could use Martinet's theorem [12], which is basically a relative version of Hunter's theorem:

Theorem 1.3 (Martinet)**.** *Let K be a number field of degree m over $\mathbb{Q}$ and let L be a finite extension of K of relative degree $n = [L : K]$. Let $\sigma_1, \ldots, \sigma_m$ denote the embeddings of K into $\mathbb{C}$. Then there exists $\alpha \in \mathcal{O}_L \backslash \mathcal{O}_K$ such that*

$$\sum_{i=1}^{mn} |\alpha_i|^2 \le \frac{1}{n} \sum_{j=1}^{m} |\sigma_j(\mathrm{Tr}_{L/K}(\alpha))|^2 + \gamma_{m(n-1)} \left(\frac{|d_L|}{n^m |d_K|} \right)^{1/m(n-1)},$$

where the α_i's are the conjugates of α, d_K is the discriminant of K, d_L is the discriminant of L, and $\gamma_{m(n-1)}$ is Hermite's constant in dimension $m(n-1)$. Furthermore, α can be chosen arbitrarily modulo addition by elements of $\mathcal{O}_K$ and also modulo multiplication by roots of unity in $\mathcal{O}_K$.

Suppose we wanted to find all fields L of degree nm containing a subfield K of degree m, and such that $|d_L| \le B$. From algebraic number theory we have

$$d_L = \pm d_K^{[L:K]} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}),$$

which implies $|d_K| \le |d_L|^{1/n} \le B^{1/n}$. So the first step in a Martinet search is to find all fields K of degree m with $|d_K| \le B^{1/n}$.

Fixing the subfield K, let α be the element coming from Martinet's theorem, and let

$$f_{\alpha,K}(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

be the minimal polynomial for α over K. The bound on $T_2(\alpha) = \sum_{i=1}^{mn} |\alpha_i|^2$ can be used to give bounds on the coefficients a_i. We omit the details of this, but it is analogous to the procedure for Hunter searches.

The general Martinet search algorithm for finding all field extensions L/K with $[L : K] = n$, $[K : \mathbb{Q}] = m$, and $|d_L| \le B$ proceeds as follows. One first finds all fields K of degree m with $|d_K| \le B^{1/n}$. For each field K, one obtains the coefficient bounds and then constructs a sequence of nested loops over these coefficients. For each combination of a_i's, one forms the polynomial $f_{\alpha,K}$. For $f_{\alpha,K}$ to be valid it must satisfy the following conditions:

1. $f_{\alpha,K}$ must be irreducible over K. When it is, we set $L = K(\alpha)$.

2. $T_2(\alpha)$ must satisfy Martinet's bound, and

3. $|d_L|$ must be less than or equal to B.

If all these conditions are met, then $f_{\alpha,K}$ is converted to a degree nm polynomial over $\mathbb{Q}$ and added to a list. The final list is refined in the exact same way that it was for the Hunter search.

As a final note, the above procedure can also be used to determine all imprimitive fields L unramified outside of a finite set of primes by first computing the bound on d_L as described in section 1.1. But as mentioned before, this approach would be highly inefficient. An efficient alternative is the targeted Martinet search, which is the subject of this dissertation.

1.3. Targeted Hunter Searches

Suppose we wanted to find all primitive number fields of degree n which are unramified outside of a finite set of primes S. As mentioned in section 1.1, the number of such fields is finite and can be found using a standard Hunter search. However, such an approach would be computationally impractical. A more practical method would be to use what is called a targeted Hunter search [7, 8].

In a targeted Hunter search, the archimedean bounds on the polynomial coefficients are the same as for a standard Hunter search. But in addition, the targeted search uses congruences on the coefficients in order to reduce the number of candidate polynomials and thereby speed up the algorithm.

A set of congruences is obtained for each possible ramification structure. Given the ramification structure, the congruences are found via a localization process at each $\mathfrak{p}$ above $p \in S$. For example, when $n = 3$ there are only 2 possible ways that p can ramify:

1. $p\mathcal{O}_K = \mathfrak{p}_1^3$, or

2. $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$.

One can show that the first ramification structure leads to a set of 2 congruences given by

$$f_\alpha(x) \equiv x^3 \pmod{p}$$

and

$$f_\alpha(x) \equiv x^3 + x^2 + \frac{1}{3}x + \left(\frac{1}{3}\right)^3 \pmod{p},$$

provided that $p \neq 3$. When $p \neq 2$, the second ramification structure leads to a set of $2p$ congruences given by

$$f_\alpha(x) \equiv x^3 - 3a^2x - 2a^3 \pmod{p}$$

and

$$f_\alpha(x) \equiv x^3 + x^2 + a(2-3a)x + a^2(1-2a) \pmod{p}$$

where $a \in \{0, 1, \ldots, p-1\}$. When $p = 2$ or 3, the ramification is wild and some additional work is required. Wild ramification gives a larger discriminant bound, but the congruences also have a larger modulus. For more detailed examples, the reader is directed to [7, 8].

1.4. Targeted Martinet Searches

The goal of my research was to combine the Martinet search technique with the targeted search technique, and apply it to the problem of finding all imprimitive fields unramified outside of a finite set of primes.

The algorithm can be viewed as having three main components. First, obtain bounds on the polynomial coefficients; second, obtain congruences on the coefficients; and third, implement the congruences. A separate chapter is devoted to each of these issues. Following that, there is a chapter giving applications of the targeted Martinet search. Finally, there is an appendix with complete tables of number fields obtained via the targeted Martinet search.

CHAPTER 2

ARCHIMEDEAN BOUNDS FOR THE COEFFICIENTS

The first component of a targeted Martinet search is to obtain decent archimedean bounds on the polynomial coefficients. Note that the bounds derived in this chapter also apply to a standard Martinet search.

Let K be a degree m field, and let L be a finite extension of K with $[L : K] = n$. Let $\sigma_1, \dots, \sigma_m$ denote the embeddings of K into $\mathbb{C}$, and for each i let $\sigma_{i1}, \dots, \sigma_{in}$ denote the embeddings of L into $\mathbb{C}$ extending σ_i. Without loss of generality, we will assume that σ_1 is the identity on K and that σ_{11} is the identity on L. Finally, we let $\omega_1, \omega_2, \dots, \omega_m$ be an integral basis for K.

Now let $\alpha \in \mathcal{O}_L \backslash \mathcal{O}_K$ be the element given by Martinet's theorem and let $f_{\alpha,K}(x) \in \mathcal{O}_K[x]$ be the minimal polynomial for α over K. Write

$$f_{\alpha,K}(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

where each $a_i \in \mathcal{O}_K$. We may also write $a_i = \sum_{j=1}^m a_{ij}\omega_j$ where each $a_{ij} \in \mathbb{Z}$.

The goal of this chapter is to give bounds for the coefficients a_i.

2.1. Bounds on a_1

According to Martinet, we may add an arbitrary element of $\mathcal{O}_K$ to α without changing the bound. The minimal polynomial for $\alpha + \sum_{j=1}^m b_j\omega_j$ is given by

$$\begin{aligned} f_\alpha\left(x - \sum_{j=1}^m b_j\omega_j\right) &= \left(x - \sum_{j=1}^m b_j\omega_j\right)^n + a_1\left(x - \sum_{j=1}^m b_j\omega_j\right)^{n-1} + \cdots + a_n \\ &= x^n + \left(a_1 - n\sum_{j=1}^m b_j\omega_j\right)x^{n-1} + \cdots. \end{aligned}$$

The x^{n-1} coefficient is

$$\sum_{j=1}^m a_{1j}\omega_j - n\sum_{j=1}^m b_j\omega_j = \sum_{j=1}^m (a_{1j} - nb_j)\,\omega_j.$$

By choosing appropriate values for b_j, we may assume that $-\lfloor \frac{n-1}{2} \rfloor \le |a_{1j}| \le \lfloor \frac{n}{2} \rfloor$ for each j. It follows that there are n^m possible values for a_1. For example, when $n = m = 2$, the possible values for a_1 are $\{0, 1, \omega, 1+\omega\}$.

But we can do better. According to Martinet, we may multiply by a root of unity in $\mathcal{O}_K$ without affecting the bound. So by choosing b_1 appropriately we first assume that $|a_{11}| \le \lfloor \frac{n}{2} \rfloor$; and then multiplying α by -1 when $a_{11} < 0$ we may assume that $a_{11} \in \{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$. Here we have used the fact that $f_{-\alpha}(x) = \pm f_\alpha(-x) = x^n - a_1 x^{n-1} + \cdots \pm a_n$. Choosing the other b_j's appropriately we may still assume that $-\lfloor \frac{n-1}{2} \rfloor \le |a_{1j}| \le \lfloor \frac{n}{2} \rfloor$ for each $j > 1$. We now have $\left(\lfloor \frac{n}{2} \rfloor + 1\right) n^{m-1}$ possible values for a_1.

But we can do still better. When $a_{11} = 0$, we may apply the same logic as above to the coefficient a_{12} to give $a_{12} \in \{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$. Similarly, when both $a_{11} = 0$ and $a_{12} = 0$, we may apply the same logic to give $a_{13} \in \{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$. And in general, when a_{11} through a_{1k} are all zero, we can assume $a_{1,k+1} \in \{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$.

Letting $\eta(n, m)$ denote the number of possible values for a_1, we have

$$\eta(n, m) = \eta(n, m-1) + \left\lfloor \frac{n}{2} \right\rfloor \cdot n^{m-1}.$$

Starting with $\eta(n, 1) = 1 + \lfloor \frac{n}{2} \rfloor$, an inductive argument gives us

$$\begin{aligned} \eta(n, m) &= 1 + \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor \cdot n + \left\lfloor \frac{n}{2} \right\rfloor \cdot n^2 + \cdots + \left\lfloor \frac{n}{2} \right\rfloor \cdot n^{m-1} \\ &= 1 + \left\lfloor \frac{n}{2} \right\rfloor \cdot (1 + n + n^2 + \cdots + n^{m-1}) \\ &= 1 + \left\lfloor \frac{n}{2} \right\rfloor \cdot \left(\frac{n^m - 1}{n - 1} \right). \end{aligned}$$

Table 2.1 gives the possible values for a_1 for various values of n and m. When $m = 2$ the table assumes the integral basis is $\{1, \omega\}$, otherwise the integral basis is $\{\omega_1, \ldots, \omega_m\}$. This table gives all possible cases for fields L with $[L : \mathbb{Q}] \le 10$.

We summarize the above results in the following theorem:

Theorem 2.1. *The coefficient a_1 can be chosen from a finite set of values. This set depends solely on n and m and contains $1 + \lfloor \frac{n}{2} \rfloor \cdot \left(\frac{n^m - 1}{n-1} \right)$ elements. Table 2.1 lists the possiblities for all degrees up to and including decics.*

Note that when $m = 1$ the above results give $\lfloor \frac{n}{2} \rfloor + 1$ possible values for a_1 given by $\{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$ which is consistent with Hunter's theorem.

Fixing the value for a_1, Martinet's bound now becomes:

$$\sum_{i=1}^{mn} |\alpha_i|^2 \le \frac{1}{n} \sum_{j=1}^{m} |\sigma_j(a_1)|^2 + \gamma_{m(n-1)} \left(\frac{|d_L|}{n^m |d_K|} \right)^{1/m(n-1)}.$$

The second term in Martinet's bound depends on the field K and the field L. Fixing the subfield K and also fixing the ramification structure for L/K, gives us values for d_K and d_L. Once these values have been fixed, we then have an actual numerical value for Martinet's bound which can be used to bound the other coefficients of f_α.

Table 2.1: The possible values for a_1 for various n and m.

n	m	$\eta(n,m)$	Possible values for a_1
2	2	4	$\{0,\ 1,\ \omega,\ 1+\omega\}$
2	3	8	$\{0,\ \omega_1,\ \omega_2,\ \omega_3,\ \omega_1{+}\omega_2,\ \omega_1{+}\omega_3,\ \omega_2{+}\omega_3,\ \omega_1{+}\omega_2{+}\omega_3\}$
2	4	16	$\left\{\sum_{i=1}^{4} a_{1i}\omega_i \;\middle|\; 0 \le a_{1i} \le 1\right\}$
2	5	32	$\left\{\sum_{i=1}^{5} a_{1i}\omega_i \;\middle|\; 0 \le a_{1i} \le 1\right\}$
3	2	5	$\{0,\ 0+\omega,\ 1,\ 1+\omega,\ 1-\omega\}$
3	3	14	$\{0,\ \omega_3,\ \omega_2,\ \omega_2-\omega_3,\ \omega_2+\omega_3,\ \omega_1,\ \omega_1-\omega_3,\ \omega_1+\omega_3,$ $\omega_1+\omega_2,\ \omega_1+\omega_2-\omega_3,\ \omega_1+\omega_2+\omega_3,\ \omega_1-\omega_2,$ $\omega_1-\omega_2-\omega_3,\ \omega_1-\omega_2+\omega_3\}$
4	2	11	$\{0,\ 0+\omega,\ 0+2\omega,\ 1,\ 1+\omega,\ 1+2\omega,\ 1-\omega,$ $2,\ 2+\omega,\ 2+2\omega,\ 2-\omega\}$
5	2	13	$\{0,\ 0+\omega,\ 0+2\omega,\ 1,\ 1+\omega,\ 1+2\omega,\ 1-2\omega,$ $1-1\omega,\ 2,\ 2+\omega,\ 2+2\omega,\ 2-2\omega,\ 2-1\omega\}$

2.2. Bounds on a_n

We now turn our attention to the constant coefficient a_n. Let C_{a_1} denote Martinet's bound where the subscript a_1 is used to signify the dependence of Martinet's bound on the coefficient a_1.

We start by considering the minimal polynomial of α over K:

$$f_{\alpha,K}(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = \prod_{j=1}^{n}(x - \sigma_{1j}(\alpha)).$$

Therefore,

$$|a_n|^2 = \prod_{j=1}^{n} |\sigma_{1j}(\alpha)|^2 \le \left[\frac{1}{n}\sum_{j=1}^{n} |\sigma_{1j}(\alpha)|^2\right]^n$$

where we have used the arithmetic/geometric mean inequality. Applying the same idea to the minimal polynomial of $\sigma_{i1}(\alpha)$ over $\sigma_i(K)$ we obtain

$$\begin{aligned} f_{\sigma_{i1}(\alpha),\sigma_i(K)} = \sigma_i(f_{\alpha,K}) &= x^n + \sigma_i(a_1)x^{n-1} + \cdots + \sigma_i(a_{n-1})x + \sigma_i(a_n) \\ &= \prod_{j=1}^{n}(x - \sigma_{ij}(\alpha)) \end{aligned}$$

and

$$|\sigma_i(a_n)|^2 = \prod_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 \le \left[\frac{1}{n}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2\right]^n.$$

Combining all these inequalities, we get

$$\begin{aligned}
\sum_{i=1}^{m} |\sigma_i(a_n)|^2 &\leq \frac{1}{n^n}\left[\sum_{j=1}^{n} |\sigma_{1j}(\alpha)|^2\right]^n + \frac{1}{n^n}\left[\sum_{j=1}^{n} |\sigma_{2j}(\alpha)|^2\right]^n \\
&\quad + \cdots + \frac{1}{n^n}\left[\sum_{j=1}^{n} |\sigma_{mj}(\alpha)|^2\right]^n \\
&\leq \frac{1}{n^n}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2\right]^n \\
&\leq \left(\frac{1}{n}C_{a_1}\right)^n. \qquad (2.1)
\end{aligned}$$

Now write $a_n = \sum_{j=1}^{m} a_{nj}\omega_j$ where each $a_{nj} \in \mathbb{Z}$. Then $\sigma_i(a_n) = \sum_{j=1}^{m} a_{nj}\sigma_i(\omega_j)$ and we get the following matrix representation

$$\begin{bmatrix} \sigma_1(a_n) \\ \sigma_2(a_n) \\ \vdots \\ \sigma_m(a_n) \end{bmatrix} = \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_m) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_m) \\ \vdots & \vdots & & \vdots \\ \sigma_m(\omega_1) & \sigma_m(\omega_2) & \cdots & \sigma_m(\omega_m) \end{bmatrix} \begin{bmatrix} a_{n1} \\ a_{n2} \\ \vdots \\ a_{nm} \end{bmatrix}.$$

Multiplying each side of this expression by its conjugate transpose, we get

$$\sum_{i=1}^{m} |\sigma_i(a_n)|^2 = \vec{a_n}^{\mathrm{H}} Q^{\mathrm{H}} Q \vec{a_n}$$

where $Q = [\sigma_i(\omega_j)]_{ij}$ and H denotes the Hermitian operator (*i.e.* conjugate transpose). We have proven the following theorem:

Theorem 2.2. *The coefficient a_n satisfies the bound*

$$\vec{a_n}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{a_n} \leq \left(\frac{1}{n}C_{a_1}\right)^n,$$

where $Q = [\sigma_i(\omega_j)]_{ij}$.

Note that the expression $\vec{a_n}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{a_n}$ is a positive definite quadratic form in the integer components of a_n.

Theorem 2.2 can be improved for the case when m is even and the signature of K is $(0, \frac{m}{2})$. Let $s = \frac{m}{2}$ and order the embeddings of K so that σ_i and σ_{i+s} are conjugate pairs $(i = 1, 2, \ldots, s)$. It follows that

$$\sum_{i=1}^{s}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 = \sum_{i=s+1}^{m}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2$$

and therefore

$$\sum_{i=1}^{s}\sum_{j=1}^{n}|\sigma_{ij}(\alpha)|^2 = \frac{1}{2}\sum_{i=1}^{m}\sum_{j=1}^{n}|\sigma_{ij}(\alpha)|^2 \le \frac{1}{2}C_{a_1}. \tag{2.2}$$

The bound in Equation 2.1 can then be made tighter as follows

$$\begin{aligned}
\sum_{i=1}^{m}|\sigma_i(a_n)|^2 &\le \frac{1}{n^n}\left[\sum_{j=1}^{n}|\sigma_{1j}(\alpha)|^2\right]^n + \cdots + \frac{1}{n^n}\left[\sum_{j=1}^{n}|\sigma_{sj}(\alpha)|^2\right]^n \\
&\quad + \frac{1}{n^n}\left[\sum_{j=1}^{n}|\sigma_{s+1,j}(\alpha)|^2\right]^n + \cdots + \frac{1}{n^n}\left[\sum_{j=1}^{n}|\sigma_{mj}(\alpha)|^2\right]^n \\
&\le \frac{1}{n^n}\left[\sum_{i=1}^{s}\sum_{j=1}^{n}|\sigma_{ij}(\alpha)|^2\right]^n + \frac{1}{n^n}\left[\sum_{i=s+1}^{m}\sum_{j=1}^{n}|\sigma_{ij}(\alpha)|^2\right]^n \\
&\le \frac{2}{n^n}\left(\frac{1}{2}C_{a_1}\right)^n.
\end{aligned}$$

We state this as a corollary.

Corollary 2.3. *Let $[K:\mathbb{Q}]$ be even and suppose K is totally complex. Then the coefficient a_n satisfies the bound*

$$\vec{a_n}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{a_n} \le \frac{1}{2^{n-1}}\left(\frac{1}{n}C_{a_1}\right)^n.$$

2.3. Bounds on a_i $(2 \le i \le n-1)$

Before bounding the other coefficients, we will need some notation. First, let $\{\alpha_1, \ldots, \alpha_n\}$ denote the roots of $f_{\alpha,K}(x)$. We then define the power sums to be

$$s_k = \sum_{j=1}^{n}\alpha_j^k$$

where $k \in \mathbb{Z}$. The power sums are inductively related to the coefficients of $f_{\alpha,K}(x)$ via Newton's formula

$$ka_k = -\sum_{j=1}^{k}a_{k-j}s_j \tag{2.3}$$

where $a_0 \stackrel{\text{def}}{=} 1$. The first few values of s_k are

$$s_1 = -a_1,$$

$$s_2 = a_1^2 - 2a_2,$$

and

$$s_3 = -a_1^3 + 3a_1a_2 - 3a_3.$$

Now define $T_k = \sum_{j=1}^{n} |\alpha_j|^k$ and note that $|s_k| \leq T_k$.

The usual strategy in the literature is to first bound s_k, and then inductively use Newton's formula to get bounds for a_k. We start by considering s_2, which may be written as

$$s_2 = \sum_{j=1}^{n} \sigma_{1j}(\alpha)^2.$$

If we apply σ_i to s_2 we get

$$\sigma_i(s_2) = \sum_{j=1}^{n} [\sigma_i \circ \sigma_{1j}(\alpha)]^2 = \sum_{j=1}^{n} \sigma_{ij}(\alpha)^2.$$

Then $|\sigma_i(s_2)| \leq \sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2$ and we get

$$\begin{aligned} \sum_{i=1}^{m} |\sigma_i(s_2)|^2 &\leq \left[\sum_{i=1}^{m} |\sigma_i(s_2)|\right]^2 \\ &\leq \left[\sum_{i=1}^{m}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2\right]^2 \\ &\leq C_{a_1}^2. \end{aligned} \tag{2.4}$$

If we let $\vec{b} = a_1^2$, then from Newton's formula we have $2\vec{a_2} = \vec{b} - \vec{s_2}$. The jth component of $\vec{a_2}$ then satisfies $a_{2j} = \frac{1}{2}(b_j - s_{2j})$. Since a_{2j} must be an integer, we only keep those values for s_{2j} having the same parity as b_j. We have proven the following theorem.

Theorem 2.4. *The power sum s_2 satisfies the bound*

$$\vec{s_2}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_2} \leq C_{a_1}^2.$$

Letting $\vec{b} = a_1^2$, the coefficient a_2 satisfies the relation

$$\vec{a_2} = \frac{1}{2}(\vec{b} - \vec{s_2}).$$

Theorem 2.4 can be improved for the case when m is even and the signature of K is $(0, \frac{m}{2})$. Let $s = \frac{m}{2}$ and order the embeddings of K so that σ_i and σ_{i+s} are conjugate pairs

$(i = 1, 2, \ldots, s)$. This time we get

$$\begin{aligned}
\sum_{i=1}^{m} |\sigma_i(s_2)|^2 &\leq \sum_{i=1}^{m} \left[\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 \right]^2 \\
&= 2 \sum_{i=1}^{s} \left[\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 \right]^2 \\
&\leq 2 \left[\sum_{i=1}^{s} \sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 \right]^2 \\
&\leq 2 \left[\frac{1}{2} C_{a_1} \right]^2 \\
&= \frac{1}{2} C_{a_1}^2
\end{aligned}$$

where we have used Equation 2.2. This gives us the following corollary.

Corollary 2.5. *Let $[K : \mathbb{Q}]$ be even and suppose K is totally complex. Then the power sum s_2 satisfies the bound*

$$\vec{s_2}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_2} \leq \frac{1}{2} C_{a_1}^2.$$

Letting $\vec{b} = a_1^2$, the coefficient a_2 satisfies the relation

$$\vec{a_2} = \frac{1}{2}(\vec{b} - \vec{s_2}).$$

The other power sums s_k can be bounded in the same way that s_2 was bounded. The precise result is stated in the following theorem.

Theorem 2.6. *The power sum s_k satisfies the bound*

$$\vec{s_k}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_k} \leq C_{a_1}^k.$$

Given a_i and s_i for $i \in \{1, 2, \ldots, k-1\}$, set $\vec{b} = -\sum_{j=1}^{k-1} a_{k-j} s_j$. Then the coefficient a_k satisfies the relation

$$\vec{a_k} = \frac{1}{k}(\vec{b} - \vec{s_k}).$$

There is a much better alternative to Theorem 2.6. The method is due to M. Pohst [14], and uses Lagrange multipliers to minimize the bounds on T_k. The method is summarized in the following theorem.

Theorem 2.7 (Pohst)**.** *Let $f = x^n + a_1 x^{n-1} + \cdots + a_n$ where a_n is fixed, let t_2 be any bound for $T_2 = \sum |\alpha_i|^2$ (the α_i's are the roots of f), and let $r = \frac{t_2}{|a_n|^{2/n}}$.*

1. *For $n_0 \in \{1, 2, \ldots, n-1\}$, the equation*

$$n_0 x^{n_0 - n} + (n - n_0) x^{n_0} = r$$

has either one or two positive roots. Let z_{n_0} be the smallest such root.

2. *For any $k \in \mathbb{Z}$, let*

$$t_k = |a_n|^{k/n} \max_{1 \le n_0 \le n-1} \left\{ n_0 z_{n_0}^{k(n_0-n)/2} + (n - n_0) z_{n_0}^{k n_0/2} \right\}.$$

Then we have the bound $|s_k| \le T_k \le t_k$.

A proof of Theorem 2.7 can be found in [3] (p.458). The next theorem is helpful for computing the z_{n_0}'s.

Theorem 2.8. *Let $R_k(x) = kx^{k-n} + (n-k)x^k$ where $1 \le k \le n-1$. For $r \ge n$, let z_k be the unique root of $R_k(x) - r = 0$ with $0 < z_k < 1$. Set $x_0 = (\frac{k}{r})^{1/(n-k)}$ and $x_{i+1} = x_i - \frac{R_k(x_i) - r}{R_k'(x_i)}$. Then x_i is an increasing sequence, $x_i < z_k$ for all i, and x_i converges quadratically to z_k.*

We will use the method of Pohst to bound $|s_k|$ for $3 \le k \le n-1$. We must apply Pohst, not only to $f_{\alpha,K}$, but also to every conjugate polynomial $f_{\sigma_{i1}(\alpha),\sigma_i(K)}$. Let $T_2^{(i)} = \sum_{j=1}^n |\sigma_{ij}(\alpha)|^2$. In order to use the method of Pohst, we need a bound $t_2^{(i)}$ for $T_2^{(i)}$. Starting from the Martinet bound $\sum_{i=1}^m \sum_{j=1}^n |\sigma_{ij}(\alpha)|^2 \le C_{a_1}$, we get

$$T_2^{(k)} = \sum_{j=1}^n |\sigma_{kj}(\alpha)|^2 \le C_{a_1} - \sum_{\substack{i=1 \\ i \ne k}}^m \sum_{j=1}^n |\sigma_{ij}(\alpha)|^2. \tag{2.5}$$

Next, from the arithmetic/geometric mean inequality we have

$$\sum_{j=1}^n |\sigma_{ij}(\alpha)|^2 \ge n \left[\prod_{j=1}^n |\sigma_{ij}(\alpha)|^2 \right]^{1/n} = n |\sigma_i(a_n)|^{2/n}.$$

Substituting this into Equation 2.5, we finally get

$$T_2^{(k)} \le C_{a_1} - n \sum_{\substack{i=1 \\ i \ne k}}^m |\sigma_i(a_n)|^{2/n}.$$

Now let $t_k^{(i)}$ be the Pohst bound for $T_k^{(i)}$, obtained by applying Pohst to the ith conjugate polynomial. We then have $|\sigma_i(s_k)| \le t_k^{(i)}$. Combining these bounds together we get

$$\vec{s_k}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_k} = \sum_{i=1}^m |\sigma_i(s_k)|^2 \le \sum_{i=1}^m \left[t_k^{(i)} \right]^2.$$

The above results are summarized in the following theorem.

Theorem 2.9. *For $k \in \{1, 2, \ldots, m\}$, let* $t_2^{(k)} = C_{a_1} - n \sum_{\substack{i=1 \\ i \neq k}}^{m} |\sigma_i(a_n)|^{2/n}$. *For each $i \in \{1, 2, \ldots, m\}$, let $\left\{ t_k^{(i)} \;\middle|\; 3 \leq k \leq n-1 \right\}$ be the Pohst bounds, obtained by applying Theorem 2.7 to $f_{\sigma_{i1}(\alpha), \sigma_i(K)}$. Set $B_{s_k} = \sum_{i=1}^{m} \left[t_k^{(i)} \right]^2$. Then the power sum s_k satisfies the bound*

$$\vec{s_k}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_k} \leq B_{s_k}.$$

Given a_i and s_i for $i \in \{1, 2, \ldots, k-1\}$, set $\vec{b} = -\sum_{j=1}^{k-1} a_{k-j} s_j$. Then the coefficient a_k satisfies the relation

$$\vec{a_k} = \frac{1}{k} (\vec{b} - \vec{s_k}).$$

2.4. Constraints on Coefficients

The bounds derived in the earlier sections are quite good. However, it is possible to augment these bounds with additional constraints on the coefficients; and any polynomial not satisfying these constraints may be discarded. We start with some lemmas. A proof for Lemma 2.10 can be found in [3] (p.452); the proofs for the other lemmas are omitted but are not difficult.

Lemma 2.10. *For $i = 1, 2, \ldots, n$ let $x_i \geq 0$, and let $k \geq 2$ be a real number. Then*

$$\sum_{i=1}^{n} x_i^k \leq \left(\sum_{i=1}^{n} x_i^2 \right)^{k/2}.$$

Lemma 2.11. *Let $n \geq 3$ and let $x_i \geq 0$ for $i = 1, 2, \ldots, n$. Then*

$$\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} x_i x_j \leq \frac{n-1}{2} \sum_{i=1}^{n} x_i^2$$

with equality iff $x_i = x_j$ for all i and j.

Lemma 2.12. *Let $n \geq 4$ and let $x_i \geq 0$ for $i = 1, 2, \ldots, n$. Then*

$$\sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} x_i x_j x_k \leq \frac{1}{6} (n-1)(n-2) \sum_{i=1}^{n} x_i^3$$

with equality iff $x_i = x_j$ for all i and j.

The next lemma generalizes the previous two lemmas.

Lemma 2.13. *Fix $k \geq 2$. Let $n \geq k+1$ and let $x_i \geq 0$ for $i = 1, 2, \ldots, n$. Then*

$$\sum \{ \text{ all distinct } k\text{-tuples } x_{i_1} x_{i_2} \cdots x_{i_k} \} \leq \frac{1}{n} \binom{n}{k} \sum_{i=1}^{n} x_i^k$$

with equality iff $x_i = x_j$ for all i and j.

2.4.1. Constraints on a_n. First consider the minimal polynomial for $-\alpha$. When n is odd,

$$f_{-\alpha}(x) = -f_\alpha(-x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots + a_{n-1}x - a_n.$$

Since $L = K(\alpha) = K(-\alpha)$, when $a_1 = 0$ we may assume $a_{n1} \geq 0$. We can do this because the bounds on a_{n1}, which come from Theorem 2.2, are symmetrical about 0.

This constraint cannot be used when n is even, because in that case $f_{-\alpha}(x)$ and $f_\alpha(x)$ have the same constant coefficient. However, a similar idea can be applied to the a_3 coefficient; this will be described in the next section.

Theorem 2.14. *If n is odd and $a_1 = 0$, then one may assume $a_{n1} \geq 0$.*

We now derive a second constraint on the a_n coefficient. Starting with the arithmetic/geometric mean inequality,

$$|\sigma_i(a_n)| = \prod_{j=1}^{n} |\sigma_{ij}(\alpha)| \leq \left[\frac{1}{n}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|\right]^n,$$

from which it follows that

$$\begin{aligned}
|\sigma_i(a_n)|^{2/n} &\leq \frac{1}{n^2}\left(\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|\right)^2 \\
&\leq \frac{1}{n^2}\left[\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 + 2\sum_{j_1=1}^{n-1}\sum_{j_2=j_1+1}^{n} |\sigma_{ij_1}(\alpha)| \cdot |\sigma_{ij_2}(\alpha)|\right] \\
&\leq \frac{1}{n^2}\left[\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 + (n-1)\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2\right] \\
&= \frac{1}{n}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2
\end{aligned}$$

where we have used Lemma 2.11. Summing over i gives

$$\sum_{i=1}^{m} |\sigma_i(a_n)|^{2/n} \leq \frac{1}{n}\sum_{i=1}^{m}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^2 \leq \frac{1}{n}C_{a_1}.$$

We have proven the following theorem.

Theorem 2.15. *The coefficient a_n satisfies the inequality*

$$\sum_{i=1}^{m} |\sigma_i(a_n)|^{2/n} \leq \frac{1}{n}C_{a_1}.$$

Theorem 2.15 can be used to give

$$\begin{aligned}\sum_{i=1}^{m}|\sigma_i(a_n)|^2 &= \sum_{i=1}^{m}\left(|\sigma_i(a_n)|^{2/n}\right)^n\\ &\leq \left(\sum_{i=1}^{m}|\sigma_i(a_n)|^{2/n}\right)^n \qquad \text{(By Lemma 2.10)}\\ &\leq \left(\frac{1}{n}C_{a_1}\right)^n\end{aligned}$$

which is the same bound derived in Theorem 2.2. So the bound of Theorem 2.15 is tighter than that of Theorem 2.2.

2.4.2. Constraints on a_k $(2 \leq k \leq n-1)$. We start with the analog of Theorem 2.14 for the case when n is even. When n is even,

$$f_{-\alpha}(x) = f_\alpha(-x) = x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots - a_{n-1}x + a_n.$$

Let $n \geq 4$ and consider the a_3 coefficient. When $a_1 = 0$, we have $s_3 = -3a_3$. Therefore, from Theorem 2.9,

$$\vec{a_3}^{\mathrm{T}}Q^{\mathrm{H}}Q\vec{a_3} = \frac{1}{9}\vec{s_3}^{\mathrm{T}}Q^{\mathrm{H}}Q\vec{s_3} \leq \frac{1}{9}B_{s_3}.$$

So we can bypass the computation for s_3, and go straight to a_3. Since the bounds on a_{31} are symmetrical about 0, we can use the same idea as in Theorem 2.14 to assume that $a_{31} \geq 0$.

Theorem 2.16. *If n is even, $n \geq 4$, and $a_1 = 0$, then a_3 satisfies the inequality*

$$\vec{a_3}^{\mathrm{T}}Q^{\mathrm{H}}Q\vec{a_3} \leq \frac{1}{9}B_{s_3}.$$

Furthermore, one may assume that $a_{31} \geq 0$.

Next, consider the a_2 coefficient. Since $a_2 = \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\sigma_{1i}(\alpha)\sigma_{1j}(\alpha)$, Lemma 2.11 gives

$$|a_2| \leq \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}|\sigma_{1i}(\alpha)|\cdot|\sigma_{1j}(\alpha)| \leq \frac{n-1}{2}\sum_{j=1}^{n}|\sigma_{1j}(\alpha)|^2.$$

We have a similar inequality for each $\sigma_i(a_2)$:

$$|\sigma_i(a_2)| \leq \frac{n-1}{2}\sum_{j=1}^{n}|\sigma_{ij}(\alpha)|^2.$$

Hence,

$$\sum_{i=1}^{m}|\sigma_i(a_2)| \leq \frac{n-1}{2}\sum_{i=1}^{m}\sum_{j=1}^{n}|\sigma_{ij}(\alpha)|^2 \leq \frac{1}{2}(n-1)C_{a_1}.$$

This proves the following theorem:

Theorem 2.17. *The coefficient a_2 satisfies the inequality*

$$\sum_{i=1}^{m} |\sigma_i(a_2)| \leq \frac{1}{2}(n-1)C_{a_1}.$$

The inequality for a_2 generalizes to the other coefficients. The coefficient a_k is the kth symmetric polynomial in the roots of $f_{\alpha,K}$. Hence,

$$a_k = \sum \{ \text{ all distinct k-tuples } \sigma_{1i_1}(\alpha)\sigma_{1i_2}(\alpha)\cdots\sigma_{1i_k}(\alpha)\}\,.$$

So from Lemma 2.13 we get

$$|a_k| \leq \frac{1}{n}\binom{n}{k}\sum_{j=1}^{n} |\sigma_{1j}(\alpha)|^k.$$

We have a similar inequality for each $\sigma_i(a_k)$:

$$|\sigma_i(a_k)| \leq \frac{1}{n}\binom{n}{k}\sum_{j=1}^{n} |\sigma_{ij}(\alpha)|^k \leq \frac{1}{n}\binom{n}{k} t_k^{(i)}$$

where $\{t_k^{(i)} \mid 1 \leq i \leq m\}$ are the Pohst bounds, obtained by applying Theorem 2.7 to $f_{\sigma_{i1}(\alpha),\sigma_i(K)}$. We have shown the following:

Theorem 2.18. *For $k \in \{3, 4, \ldots, n-1\}$, the coefficient a_k simultaneously satisfies the following m inequalities:*

$$|\sigma_i(a_k)| \leq \frac{1}{n}\binom{n}{k} t_k^{(i)} \qquad (1 \leq i \leq m)$$

where $\{t_k^{(i)} \mid 1 \leq i \leq m\}$ are the Pohst bounds.

In particular, Theorem 2.18 gives

$$|\sigma_i(a_3)| \leq \frac{1}{6}(n-1)(n-2)t_3^{(i)},$$

$$|\sigma_i(a_4)| \leq \frac{1}{24}(n-1)(n-2)(n-3)t_4^{(i)}.$$

At first sight, these bounds might appear to be too loose to be helpful, but experience shows this is not the case, especially for small n. For example, when $n = 5$, the second inequality becomes $|\sigma_i(a_4)| \leq t_4^{(i)}$, which is actually quite good.

2.4.3. Constraints on a_{n-1}. In addition to the constraint on a_{n-1} given in the previous section, there is another useful constraint which can be applied when $n \geq 5$, which is now described.

A careful reading of Theorem 2.7 tells us that the method of Pohst also applies to $T_{-1} \stackrel{\text{def}}{=} \sum_i |\alpha_i|^{-1}$. Letting $t_{-1}^{(i)}$ be the Pohst bound corresponding to the ith conjugate polynomial, we have $|\sigma_i(s_{-1})| \leq t_{-1}^{(i)}$. If we let α_1,α_2,…,α_n denote the roots of $f_{\alpha,K}$, then the a_n and a_{n-1} coefficients are given by:

$$a_n = (-1)^n \prod_{i=1}^{n} \alpha_i,$$

$$a_{n-1} = (-1)^{n+1} \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} \alpha_j.$$

Therefore,

$$-\frac{a_{n-1}}{a_n} = \sum_{i=1}^{n} \frac{1}{\alpha_i} = s_{-1}$$

which implies $|a_{n-1}| = |s_{-1}a_n| \leq t_{-1}^{(1)}|a_n|$. The same argument can be applied to the conjugate polynomials, which gives $|\sigma_i(a_{n-1})| \leq t_{-1}^{(i)}|\sigma_i(a_n)|$. We now have the following theorem:

Theorem 2.19. *Let $n \geq 5$. Then given a_n, the coefficient a_{n-1} simultaneously satisfies the following m inequalities:*

$$|\sigma_i(a_{n-1})| \leq t_{-1}^{(i)}|\sigma_i(a_n)| \qquad (1 \leq i \leq m)$$

where $\{t_{-1}^{(i)} \mid 1 \leq i \leq m\}$ are the Pohst bounds.

2.4.4. Additional Constraints. Another set of constraints can be derived by applying the method of Pohst to the characteristic polynomial of α over $\mathbb{Q}$. Let $c_\alpha(x)$ denote this characteristic polynomial, which is the product of all the conjugate polynomials:

$$c_\alpha(x) = \prod_{i=1}^{m} f_{\sigma_{i1}(\alpha),\sigma_i(K)}(x).$$

The polynomial $c_\alpha(x)$ has integer coefficients and $f_{\alpha,\mathbb{Q}} \mid c_\alpha$. In some applications, we may assume $c_\alpha = f_{\alpha,\mathbb{Q}}$, but in general this is not the case.

Since the roots of $c_\alpha(x)$ are the $\sigma_{ij}(\alpha)$'s, it follows that the roots of c_α satisfy Martinet's bound. Also, the constant coefficient of c_α is $\prod_{i=1}^{m} \sigma_i(a_n) = \mathrm{N}_{K/\mathbb{Q}}(a_n)$. So we have everything we need in order to apply the method of Pohst to the polynomial c_α.

If we write $c_\alpha(x) = \sum_{i=0}^{nm} b_i x^{nm-i}$, then we have the following constraint on b_2

$$\left\lceil \frac{1}{2}(b_1^2 - C_{a_1}) \right\rceil \leq b_2 \leq \left\lfloor \frac{1}{2}(b_1^2 + C_{a_1}) \right\rfloor.$$

This comes from the fact that $|b_1^2 - 2b_2| = |s_2| \leq C_{a_1}$. As shown in [3] (p.451), the Cauchy-Schwartz inequality can be used to improve this bound, giving

$$\left\lceil \frac{1}{2}(b_1^2 - C_{a_1}) \right\rceil \leq b_2 \leq \left\lfloor \frac{1}{2}\left(\frac{nm-2}{nm} b_1^2 + C_{a_1}\right) \right\rfloor. \tag{2.6}$$

Let t_i denote the Pohst bounds for c_α. The analog of Theorem 2.19 gives the following bounds on b_{nm-1}:

$$-|b_{nm}t_{-1}| \leq b_{nm-1} \leq |b_{nm}t_{-1}|. \tag{2.7}$$

Constraints can also be obtained for the other b_i's in an inductive manner using Newton's formulas. Since $|s_k| \leq t_k$ and $s_k = -kb_k - \sum_{j=1}^{k-1} b_{k-j}s_j$ we get the following bounds on b_k:

$$\left\lceil \frac{-t_k - \sum_{j=1}^{k-1} b_{k-j}s_j}{k} \right\rceil \leq b_k \leq \left\lfloor \frac{t_k - \sum_{j=1}^{k-1} b_{k-j}s_j}{k} \right\rfloor. \tag{2.8}$$

Since the b_i's are functions of the coefficients of $f_{\alpha,K}$, the above bounds translate into a set of relations between the a_i's. The exact form of these relations depends on the specific case, as seen in the following example.

Example 2.1. *Suppose we are interested in decics having a quadratic subfield, so that $n = 5$ and $m = 2$. Letting $a_i^* = \sigma_2(a_i)$, we have*

$$\begin{aligned} c_\alpha(x) &= (x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5) \times (x^5 + a_1^*x^4 + a_2^*x^3 + a_3^*x^2 + a_4^*x + a_5^*) \\ &= x^{10} + (a_1 + a_1^*)x^9 + (a_1a_1^* + a_2 + a_2^*)x^8 + (a_1a_2^* + a_1^*a_2 + a_3 + a_3^*)x^7 \\ &\quad +(a_1a_3^* + a_1^*a_3 + a_2a_2^* + a_4 + a_4^*)x^6 + (a_1a_4^* + a_1^*a_4 + a_2a_3^* + a_2^*a_3 + a_5 + a_5^*)x^5 \\ &\quad +(a_1a_5^* + a_1^*a_5 + a_2a_4^* + a_2^*a_4 + a_3a_3^*)x^4 + (a_2a_5^* + a_2^*a_5 + a_3a_4^* + a_3^*a_4)x^3 \\ &\quad +(a_3a_5^* + a_3^*a_5 + a_4a_4^*)x^2 + (a_4a_5^* + a_4^*a_5)x + a_5a_5^*. \end{aligned} \tag{2.9}$$

Writing this polynomial as $c_\alpha(x) = \sum_{i=0}^{10} b_ix^{10-i}$, Equation 2.6 gives the following relation:

$$\left\lceil \frac{1}{2}((a_1 + a_1^*)^2 - C_{a_1}) \right\rceil \leq (a_1a_1^* + a_2 + a_2^*) \leq \left\lfloor \frac{1}{2}\left(\frac{4}{5}(a_1 + a_1^*)^2 + C_{a_1}\right) \right\rfloor.$$

Likewise, Equation 2.7 gives another relation:

$$-|(a_5a_5^*)t_{-1}| \leq (a_4a_5^* + a_4^*a_5) \leq |(a_5a_5^*)t_{-1}|.$$

Finally, Equation 2.8 can be used inductively to give a relation for each coefficient in the decic of Equation 2.9.

Experience shows that incorporating these constraints into the algorithm can lead to substantial speed improvement, sometimes an order of magnitude faster.

CHAPTER 3

COMPUTING CONGRUENCE VECTORS

An important part of any targeted search, either Hunter or Martinet, is to obtain all possible congruences on the polynomial coefficients. The congruences for a Martinet search are obtained in a similar fashion to those of the Hunter search; in fact, the method used to find the Martinet congruences can be viewed as a generalization of the Hunter method. For Martinet, the method is a little more complicated because the congruences are modulo an ideal, whereas the Hunter congruences are modulo an integer.

As usual, we let K be a degree m field and we let L be a finite extension of K with $[L:K]=n$. Let $\alpha \in \mathcal{O}_L \backslash \mathcal{O}_K$ be the element given by Martinet's theorem and let $f_{\alpha,K}(x) \in \mathcal{O}_K[x]$ be the minimal polynomial for α over K. This minimal polynomial will also be denoted f_α, where it is understood to be over K (not $\mathbb{Q}$).

Recall that we wish to obtain those field extensions L/K which are unramified outside of a finite set of primes S. Let S_K denote the set of prime ideals of $\mathcal{O}_K$ which lie above any prime in S. The goal of this chapter is to show how to obtain all possible congruences of f_α modulo $\mathfrak{p}$ where $\mathfrak{p} \in S_K$.

We will first discuss how the problem can be reduced from the global realm to the local realm. We then show how to obtain the congruences in the local case. Finally, we will show how the wildly ramified case can be handled more carefully to give congruences modulo a power of $\mathfrak{p}$.

3.1. The Global to Local Principle

Fix a prime ideal $\mathfrak{p} \in S_K$ and let $p \in S$ be the prime below $\mathfrak{p}$. There are only a finite number of ways in which $\mathfrak{p}$ may ramify in L, and we need to obtain a set of congruences for each of these ramification structures. Let us target a specific ramification structure, say $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$.

Let $K_\mathfrak{p}$ be the completion of K with respect to $\mathfrak{p}$, and let L_i be the completion of L with respect to $\mathfrak{P}_i$ $(i = 1, \ldots, g)$. Let $\mathcal{O}_{K_\mathfrak{p}}$ and $\mathcal{O}_{L_i}$ be the corresponding rings of integers; and let $\mathcal{P}_{K_\mathfrak{p}}$ and $\mathcal{P}_{L_i}$ be the unique maximal ideals.

We know from algebraic number theory that f_α has a factorization over $K_\mathfrak{p}$ with g irreducible factors, say $f_\alpha = f_1 \cdots f_g$. It will be shown in the next several sections how one may obtain congruences for each f_i modulo $\mathcal{P}_{K_\mathfrak{p}}^k$ $(k \geq 1)$. The following simple theorem shows how one may combine these individual congruences into a single congruence for f_α modulo $\mathfrak{p}^k$.

Theorem 3.1. *Suppose f_α factors over $K_\mathfrak{p}$ into irreducibles as*

$$f_\alpha(x) = f_1(x) \cdots f_g(x).$$

Also suppose that for each i, $f_i(x) \equiv h_i(x) \pmod{\mathcal{P}_{K_\mathfrak{p}}^k}$ for some $k \geq 1$ and where each $h_i \in \mathcal{O}_K[x]$. Then

$$f_\alpha(x) \equiv h_1(x) \cdots h_g(x) \pmod{\mathfrak{p}^k}.$$

Proof. We may write $\prod h_i = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n$ where each $b_i \in \mathcal{O}_K$. Then

$$\begin{aligned} f_\alpha(x) &= x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \\ &\equiv x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n \pmod{\mathcal{P}_{K_\mathfrak{p}}^k}. \end{aligned}$$

Therefore, $a_i - b_i \in \mathcal{P}_{K_\mathfrak{p}}^k \cap \mathcal{O}_K = \mathfrak{p}^k$ for every i. It follows that $f_\alpha(x) \equiv h_1(x) \cdots h_g(x) \pmod{\mathfrak{p}^k}$. □

Equipped with this theorem, we only have left to consider the local case. This will be the subject of the remaining sections; but before that, we make some remarks. First, if N_i is the number of congruences for f_i, then the number of congruences for f_α will be $\prod N_i$. However, this number can be reduced by keeping only those congruences whose first coefficient is one of the allowed values as given by Theorem 2.1.

Next, the congruences modulo $\mathcal{P}_{K_\mathfrak{p}}^k$ for $k > 1$ correspond to wildly ramified cases; tamely ramified cases will always have $k = 1$. When at least one factor f_i has a congruence with $k > 1$, we increase the moduli for all factors to the maximum k. We now describe how this is done.

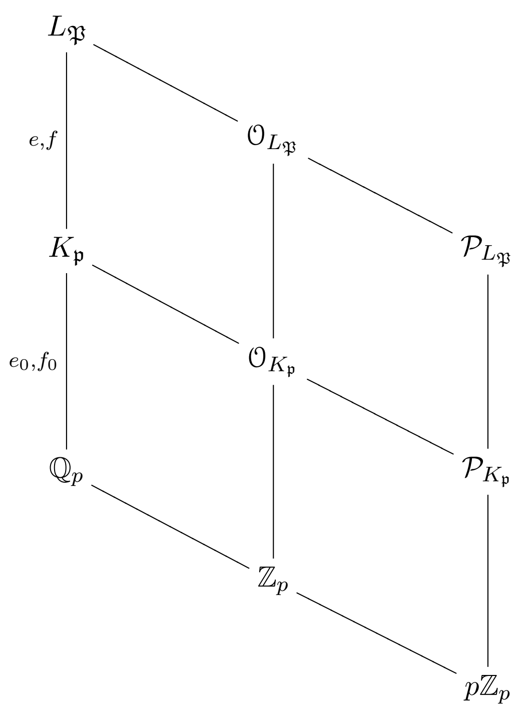
Let $\Gamma \subseteq \mathcal{O}_K$ be a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$. Then Γ is also a complete set of representatives for $\mathcal{O}_{K_\mathfrak{p}}/\mathcal{P}_{K_\mathfrak{p}}$; because if $\gamma_i + \mathcal{P}_{K_\mathfrak{p}} = \gamma_j + \mathcal{P}_{K_\mathfrak{p}}$ then $\gamma_i - \gamma_j \in \mathcal{P}_{K_\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{p}$ which means $i = j$. Next, let $\rho \in \mathfrak{p} \backslash \mathfrak{p}^2$. Then $\rho \in \mathcal{P}_{K_\mathfrak{p}} \backslash \mathcal{P}_{K_\mathfrak{p}}^2$ is a uniformizer for $\mathcal{O}_{K_\mathfrak{p}}$. From algebraic number theory, we know that any $B \in \mathcal{O}_{K_\mathfrak{p}}$ may be written as a power series in ρ with coefficients from the set Γ.

Now suppose we have a congruence modulo $\mathcal{P}_{K_\mathfrak{p}}^{k_1}$ which we would like to increase to $\mathcal{P}_{K_\mathfrak{p}}^{k_2}$ ($k_2 > k_1$). Let $B \in \mathcal{O}_K$ represent a single coefficient for this congruence. Then B will have the form

$$\begin{aligned} B &= b_0 + b_1\rho + b_2\rho^2 + \cdots \\ &\equiv b_0 + b_1\rho + b_2\rho^2 + \cdots + b_{k_1-1}\rho^{k_1-1} \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_1}} \\ &\equiv b_0 + b_1\rho + b_2\rho^2 + \cdots + b_{k_2-1}\rho^{k_2-1} \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_2}} \end{aligned}$$

where each $b_i \in \Gamma$. So to change from modulus $\mathcal{P}_{K_\mathfrak{p}}^{k_1}$ to modulus $\mathcal{P}_{K_\mathfrak{p}}^{k_2}$, it suffices to just tack on a few more terms to the power series expansion. Note that increasing the modulus

Figure 3.1: Local field diagram.



power in this fashion will also increase the final number of congruences; however, the added benefit of the larger modulus far outweighs the extra congruences.

As a final remark, when $\mathfrak{p}$ is unramified at $\mathfrak{P}_i$ (*i.e.* $e_i = 1$), the corresponding factor $f_i(x)$ will be an arbitrary degree f polynomial, where f is the residue class degree of $\mathfrak{P}_i$ over $\mathfrak{p}$. Therefore, all possible degree f congruences will be present. In other words, the set of congruences will be $\{x^f + \gamma_{f-1}x^{f-1} + \cdots + \gamma_1 x + \gamma_0 \mid \gamma_j \in \Gamma\}$. So from here on we only need to consider the ramified case.

3.2. Local Congruences

As shown in the previous section, the problem of finding the congruences for f_α is reduced to the local realm. As before, fix $\mathfrak{p} \in S_K$ and let $p \in S$ be the prime below $\mathfrak{p}$. Let $\mathfrak{P}$ be a fixed prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$ with ramification index $e = e(\mathfrak{P}/\mathfrak{p})$ and residue class degree $f = f(\mathfrak{P}/\mathfrak{p})$. As mentioned in the previous section, it suffices to assume that $e > 1$. Next, let $e_0 = e(\mathfrak{p}/p\mathbb{Z})$ and $f_0 = f(\mathfrak{p}/p\mathbb{Z})$. Let $K_{\mathfrak{p}}$ be the completion of K with respect to $\mathfrak{p}$, and let $L_{\mathfrak{P}}$ be the completion of L with respect to $\mathfrak{P}$. Let $\mathcal{O}_{K_{\mathfrak{p}}}$ and $\mathcal{O}_{L_{\mathfrak{P}}}$ be the rings of integers for $K_{\mathfrak{p}}$ and $L_{\mathfrak{P}}$ respectively; and let $\mathcal{P}_{K_{\mathfrak{p}}}$ and $\mathcal{P}_{L_{\mathfrak{P}}}$ be the unique maximal ideals. The local field diagram is displayed in Figure 3.1.

Recall that f_α factors over $K_{\mathfrak{p}}$ into irreducibles that are in one to one correspondence with the primes of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Let $f_{\mathfrak{P}}(x)$ denote the factor of f_α corresponding to

$\mathfrak{P}$. In order to use Theorem 3.1, we need to obtain congruences for $f_{\mathfrak{P}}(x)$ modulo a power of $\mathcal{P}_{K_{\mathfrak{p}}}$.

We note that $L_{\mathfrak{P}} = K_{\mathfrak{p}}[x]/\langle f_{\mathfrak{P}}\rangle$ and that $L_{\mathfrak{P}} = K_{\mathfrak{p}}(\eta)$ where η is a root of $f_{\mathfrak{P}}(x)$. Now since $f_\alpha \in \mathcal{O}_{K_{\mathfrak{p}}}[x]$ is monic and $\mathcal{O}_{K_{\mathfrak{p}}}$ is a UFD, by Gauss' Lemma we may assume that $f_{\mathfrak{P}} \in \mathcal{O}_{K_{\mathfrak{p}}}[x]$. Therefore, since $\mathcal{O}_{L_{\mathfrak{P}}}$ is the integral closure of $\mathcal{O}_{K_{\mathfrak{p}}}$, it follows that $\eta \in \mathcal{O}_{L_{\mathfrak{P}}}$.

3.2.1. The Totally Ramified Case. In this subsection we consider the case when $f = 1$. This simplifies the analysis immensely. Since $\left[\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{P}_{L_{\mathfrak{P}}} : \mathcal{O}_{K_{\mathfrak{p}}}/\mathcal{P}_{K_{\mathfrak{p}}}\right] = 1$, we have

$$\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{P}_{L_{\mathfrak{P}}} \cong \mathcal{O}_{K_{\mathfrak{p}}}/\mathcal{P}_{K_{\mathfrak{p}}} \cong \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^{f_0}}.$$

Let $\Gamma = \left\{\gamma_1, \gamma_2, \ldots, \gamma_{p^{f_0}}\right\} \subseteq \mathcal{O}_K$ be a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$. Then Γ is also a complete set of representatives for $\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{P}_{L_{\mathfrak{P}}}$. In particular, we have

$$\mathcal{O}_{L_{\mathfrak{P}}} = \bigcup_{i=1}^{p^{f_0}} \left(\gamma_i + \mathcal{P}_{L_{\mathfrak{P}}}\right). \tag{3.1}$$

Let $\beta \in \mathcal{P}_{L_{\mathfrak{P}}}$ and let $c_\beta(x)$ be the characteristic polynomial for β over $K_{\mathfrak{p}}$. Then $|\beta_i|_p = |\beta|_p < 1$ for all conjugates β_i of β. Since the coefficients of the minimal polynomial for β over $K_{\mathfrak{p}}$ are symmetric polynomials in the β_i's it follows that $c_\beta(x) \equiv x^e \pmod{\mathcal{P}_{K_{\mathfrak{p}}}}$.

Next, according to Equation 3.1, any element $\beta \in \mathcal{O}_{L_{\mathfrak{P}}}$ is a translate by some $\gamma \in \Gamma$ of an element in $\mathcal{P}_{L_{\mathfrak{P}}}$. Therefore, $c_\beta(x) \equiv (x+\gamma)^e \pmod{\mathcal{P}_{K_{\mathfrak{p}}}}$. In particular, $f_{\mathfrak{P}}(x)$ satisfies this congruence because $f_{\mathfrak{P}}$ is the minimal polynomial for $\eta \in \mathcal{O}_{L_{\mathfrak{P}}}$. This proves the following theorem.

Theorem 3.2. *Let $\Gamma \subseteq \mathcal{O}_K$ be a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$ and suppose $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is totally ramified with ramification index e. Then*

$$f_{\mathfrak{P}}(x) \equiv (x+\gamma)^e \pmod{\mathcal{P}_{K_{\mathfrak{p}}}}$$

for some $\gamma \in \Gamma$.

Note that Theorem 3.2 gives a maximum of $|\Gamma| = p^{f_0}$ different congruences for $f_{\mathfrak{P}}(x)$.

3.2.2. The $f > 1$ Case. As in the previous section, we have

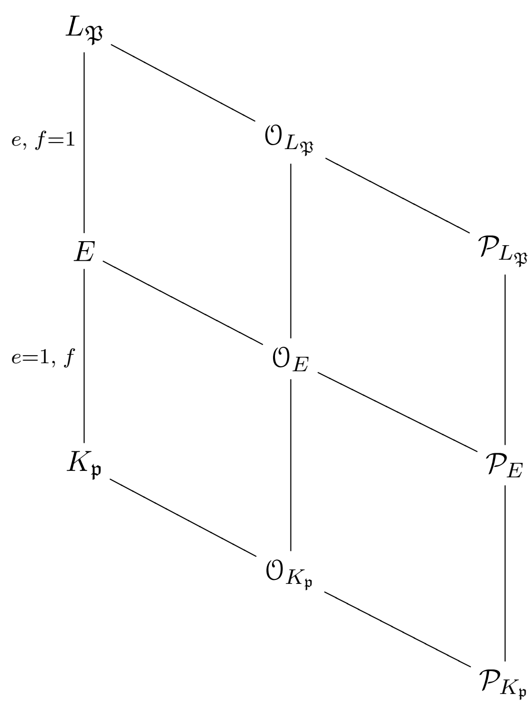
$$\mathcal{O}_{K_{\mathfrak{p}}}/\mathcal{P}_{K_{\mathfrak{p}}} \cong \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^{f_0}},$$

and we let $\Gamma \subseteq \mathcal{O}_K$ be a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$. Then Γ is also a complete set of representatives for $\mathcal{O}_{K_{\mathfrak{p}}}/\mathcal{P}_{K_{\mathfrak{p}}}$. This time, $\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{P}_{L_{\mathfrak{P}}}$ is a degree f extension of $\mathcal{O}_{K_{\mathfrak{p}}}/\mathcal{P}_{K_{\mathfrak{p}}}$, hence

$$\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{P}_{L_{\mathfrak{P}}} \cong \mathbb{F}_{p^{f \cdot f_0}}.$$

From algebraic number theory, we know there exists an intermediate field E, $K_{\mathfrak{p}} \subseteq E \subseteq L_{\mathfrak{P}}$ such that $L_{\mathfrak{P}}/E$ is totally ramified and $E/K_{\mathfrak{p}}$ is unramified. The modified local field diagram is displayed in Figure 3.2.

FIGURE 3.2: Local field diagram showing the intermediate field E.



Now let $\hat{\Gamma} \subseteq \mathcal{O}_E$ be a complete set of representatives for $\mathcal{O}_E/\mathcal{P}_E$. Then $\hat{\Gamma}$ is also a complete set of representatives for $\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{P}_{L_{\mathfrak{P}}}$. Also, since $\mathcal{O}_E$ is the integral closure of $\mathcal{O}_{K_{\mathfrak{p}}}$, any $\hat{\gamma} \in \hat{\Gamma}$ has characteristic polynomial over $K_{\mathfrak{p}}$ satisfying

$$c_{\hat{\gamma},K_{\mathfrak{p}}}(x) \equiv x^f + \gamma_1 x^{f-1} + \cdots + \gamma_{f-1}x + \gamma_f \pmod{\mathcal{P}_{K_{\mathfrak{p}}}} \tag{3.2}$$

for some $\gamma_1, \ldots, \gamma_f \in \Gamma$.

Before proceeding, we will need some more notation. Let $\sigma_1, \ldots, \sigma_f$ denote the embeddings of E (fixing $K_{\mathfrak{p}}$) into an algebraic closure of $L_{\mathfrak{P}}$, and for each i let $\{\sigma_{i1}, \ldots, \sigma_{ie}\}$ denote the embeddings of $L_{\mathfrak{P}}$ extending σ_i. Without loss of generality, we will assume that σ_1 is the identity on E and that σ_{11} is the identity on $L_{\mathfrak{P}}$. Since $E/K_{\mathfrak{p}}$ is unramified, it is necessarily Galois, and therefore $\sigma_i(E) = E$ for each i. Finally, we let $\beta_{ij} = \sigma_{ij}(\beta)$ denote the conjugates of any element $\beta \in L_{\mathfrak{P}}$.

Any element $\beta \in \mathcal{P}_{L_{\mathfrak{P}}}$ has characteristic polynomial over E satisfying $c_{\beta,E}(x) \equiv x^e$ modulo $\mathcal{P}_E$. Now let $\beta \in \mathcal{O}_{L_{\mathfrak{P}}}$. Then β is a translate by some $\hat{\gamma} \in \hat{\Gamma}$ of an element in $\mathcal{P}_{L_{\mathfrak{P}}}$. Therefore,

$$c_{\beta,E}(x) \equiv (x - \hat{\gamma})^e \pmod{\mathcal{P}_E} \tag{3.3}$$

where the characteristic polynomial of $\hat{\gamma}$ satisfies Equation 3.2.

Now write $c_{\beta,E}(x) = x^e + d_1 x^{e-1} + \cdots + d_{e-1}x + d_e$, where each $d_i \in \mathcal{O}_E$. The characteristic polynomial for the conjugate β_{i1} is given by

$$\begin{aligned} c_{\beta_{i1},E}(x) &= x^e + \sigma_i(d_1)x^{e-1} + \cdots + \sigma_i(d_{e-1})x + \sigma_i(d_e) \\ &= \sigma_i(c_{\beta,E}(x)) \\ &\equiv \sigma_i([x-\hat{\gamma}]^e) \pmod{\mathcal{P}_E} \\ &= [x - \sigma_i(\hat{\gamma})]^e. \end{aligned}$$

Finally, the characteristic polynomial for β over $K_{\mathfrak{p}}$ is given by

$$\begin{aligned} c_{\beta,K_{\mathfrak{p}}}(x) &= \prod_{i=1}^{f}\prod_{j=1}^{e}[x-\beta_{ij}] \\ &= \prod_{i=1}^{f} c_{\beta_{i1},E}(x) \\ &\equiv \prod_{i=1}^{f}[x-\sigma_i(\hat{\gamma})]^e \pmod{\mathcal{P}_E} \\ &= \left(\prod_{i=1}^{f}[x-\sigma_i(\hat{\gamma})]\right)^e \\ &= \left[c_{\hat{\gamma},K_{\mathfrak{p}}}(x)\right]^e \\ &\equiv \left(x^f + \gamma_1 x^{f-1} + \cdots + \gamma_{f-1}x + \gamma_f\right)^e \pmod{\mathcal{P}_{K_{\mathfrak{p}}}}. \end{aligned}$$

Note that $f_{\mathfrak{P}}(x)$ satisfies a congruence of this type because $f_{\mathfrak{P}}$ is the minimal polynomial for $\eta \in \mathcal{O}_{L_{\mathfrak{P}}}$. We have proven the following theorem.

Theorem 3.3. *Let $\Gamma \subseteq \mathcal{O}_K$ be a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$, and let e, f be the ramification index and residue class degree respectively for $\mathcal{P}_{L_{\mathfrak{P}}}$ over $\mathcal{P}_{K_{\mathfrak{p}}}$. Then*

$$f_{\mathfrak{P}}(x) \equiv \left(x^f + \gamma_1 x^{f-1} + \cdots + \gamma_{f-1}x + \gamma_f\right)^e \pmod{\mathcal{P}_{K_{\mathfrak{p}}}}$$

for some $\gamma_1, \ldots, \gamma_f \in \Gamma$.

Note that Theorem 3.3 is a generalization of Theorem 3.2. It gives a maximum of $|\Gamma|^f = p^{f_0 f}$ different congruences for $f_{\mathfrak{P}}(x)$. Since we will be interested in applications with L no larger than degree 10 (*i.e.* $[L:K] \leq 5$), the largest residue class degree we will see is $f = 2$.

3.3. Wild Ramification

The congruences derived in the previous section still hold for the wildly ramified case. However, when p divides e, we can improve algorithm efficiency by replacing these congruences with new ones modulo a power of $\mathcal{P}_{K_{\mathfrak{p}}}$. In some applications, these larger moduli are essential; without them, the algorithm could take months or even years to complete.

We start by introducing the concept of the Newton-Ore exponents. This terminology originated with [7]. The reason for using the name Newton-Ore is because of the connection to both Newton polygons and Ore's formulas for discriminants of Eisenstein polynomials [13].

Let $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ be totally ramified, let ρ be a uniformizer for $K_{\mathfrak{p}}$, and let π be a uniformizer for $L_{\mathfrak{P}}$. Write the minimal polynomial for π over $K_{\mathfrak{p}}$ as

$$f_\pi(x) = x^e + a_1x^{e-1} + a_2x^{e-2} + \cdots + a_{e-2}x^2 + a_{e-1}x + a_e$$

where each $a_i \in \mathcal{O}_{K_{\mathfrak{p}}}$. Write $a_i = \rho^{d_i}a_i'$ where $(\rho, a_i') = 1$. Since $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is totally ramified, f_π must be Eisenstein, and therefore $d_i \geq 1$ for all i and $d_e = 1$. Since f_π is monic, we may also define $a_0 = 1$ and $d_0 = 0$.

Let D denote the exponent of $\mathcal{P}_{L_{\mathfrak{P}}}$ in $\mathcal{D}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Then

$$D = \nu_\pi(f_\pi'(\pi)) = \nu_\pi(e\pi^{e-1} + (e-1)a_1\pi^{e-2} + \cdots + 2a_{e-2}\pi + a_{e-1}). \tag{3.4}$$

Since $\nu_\pi(\rho) = e$, we get

$$\nu_\pi(a) = e\nu_\rho(a) \qquad \forall a \in \mathcal{O}_{K_{\mathfrak{p}}}.$$

Consequently, for $0 \leq k \leq e-1$, we have

$$\nu_\pi((e-k)a_k\pi^{e-k-1}) = ed_k + e - (k+1) + e\nu_\rho(e-k).$$

For $0 \leq k \leq e-1$, define

$$D_k = ed_k + e - (k+1) + e\nu_\rho(e-k). \tag{3.5}$$

One observes that the D_k's are distinct modulo e, hence distinct in $\mathbb{Z}^+$. Therefore, the valuation in Equation 3.4 is equal to the minimum of the individual valuations and we get

$$D = \nu_\pi(e\pi^{e-1} + (e-1)a_1\pi^{e-2} + \cdots + 2a_{e-2}\pi + a_{e-1}) = \min_{0\leq i\leq e-1}\{D_i\}.$$

To simplify the equations to come, we make a definition. If s represents any statement which can be either true or false, then we define δ_s to be 1 if s is true, and 0 otherwise. For example,

$$\delta_{j>k} = \begin{cases} 1 & \text{if } j > k \\ 0 & \text{if } j \leq k \end{cases}.$$

Suppose $\min_{0\leq i\leq e-1}\{D_i\} = D_k$. Then from Equation 3.5, the exponent d_k is forced to be

$$d_k = \frac{1}{e}\left[D - e + (k+1) - e\nu_\rho(e-k)\right].$$

For $j \neq k$ and $j \neq e$ we have $D_j > D_k$. Therefore,

$$ed_j + e - (j+1) + e\nu_\rho(e-j) > ed_k + e - (k+1) + e\nu_\rho(e-k).$$

$$\implies ed_j > ed_k + j - k + e\nu_\rho(e-k) - e\nu_\rho(e-j)$$
$$\implies d_j > d_k + \frac{j-k}{e} + \nu_\rho(e-k) - \nu_\rho(e-j)$$

Since every term in the last equation is an integer except for the $(j-k)/e$ term, this becomes

$$d_j \geq \begin{cases} d_k + 1 + \nu_\rho(e-k) - \nu_\rho(e-j) & \text{if } j > k \\ d_k + \nu_\rho(e-k) - \nu_\rho(e-j) & \text{if } j < k \end{cases}, \tag{3.6}$$

and since $d_j \geq 1$, we get

$$d_j \geq \max\{d_k + \delta_{j>k} + \nu_\rho(e-k) - \nu_\rho(e-j), 1\}. \tag{3.7}$$

Since $d_e = 1$, we see that Equation 3.7 is also valid for $j = e$.

Recall that we want the Newton-Ore exponents to be the smallest possible exponents. This motivates the next definition.

Definition 3.4. *If the exponent of $\mathcal{P}_{L_\mathfrak{P}}$ in $\mathcal{D}(L_\mathfrak{P}/K_\mathfrak{p})$ is $D = D_k$, then the* **Newton-Ore exponents** $(c_1, \ldots, c_e)$*, are defined as*

1. $c_k = \frac{1}{e}\left[D - e + (k+1) - e\nu_\rho(e-k)\right]$*, and*
2. *for $1 \leq j \leq e$, $j \neq k$*

$$c_j = \max\{c_k + \delta_{j>k} + \nu_\rho(e-k) - \nu_\rho(e-j), 1\}.$$

We say that $\beta \in \mathcal{P}_{L_\mathfrak{P}}$ satisfies the **Newton-Ore exponent condition** *if $\nu_\rho(b_i) \geq c_i$ for every i, where the b_i are the coefficients of the characteristic polynomial for β.*

The above analysis implies that any uniformizer for $L_\mathfrak{P}$ satisfies the Newton-Ore exponent condition. The next theorem says that this is also the case for any element of $\mathcal{P}_{L_\mathfrak{P}}$. This theorem will be crucial in the analysis to come.

Theorem 3.5. *Let $L_\mathfrak{P}/K_\mathfrak{p}$ be totally ramified. Then any $\alpha \in \mathcal{P}_{L_\mathfrak{P}}$ satisfies the Newton-Ore exponent condition.*

Proof. See Chapter 4. □

To simplify the analysis, we handle each extension degree separately. But first we define some notation that will be common among all cases. Let $\rho \in \mathfrak{p}\backslash\mathfrak{p}^2$. Then $\rho \in \mathcal{P}_{K_\mathfrak{p}}\backslash\mathcal{P}_{K_\mathfrak{p}}^2$, so it is a uniformizer for $\mathcal{O}_{K_\mathfrak{p}}$. Next, let $\pi \in \mathcal{P}_{L_\mathfrak{P}}\backslash\mathcal{P}_{L_\mathfrak{P}}^2$ be a uniformizer for $L_\mathfrak{P}$ and let d be the exponent of $\mathcal{P}_{L_\mathfrak{P}}$ in $\mathcal{D}(L_\mathfrak{P}/K_\mathfrak{p})$ (this is what we called D above). Finally, let $\Gamma \subseteq \mathcal{O}_K$ be a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$. Then Γ is also a complete set of representatives for $\mathcal{O}_{K_\mathfrak{p}}/\mathcal{P}_{K_\mathfrak{p}}$, and also for $\mathcal{O}_{L_\mathfrak{P}}/\mathcal{P}_{L_\mathfrak{P}}$ when $f = 1$.

Since all applications that we will consider will have $[L : K] \leq 5$, we may assume $f = 1$, except for the quartic case, for which $f = 2$ is also a possibility.

3.3.1. Quadratic Extensions. Here we assume $e = 2$ and $f = 1$. Also, for $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ to be wildly ramified we must assume that $p = 2$.

For this case we have

$$f_\pi(x) = x^2 + a_1 x + a_2 \in \mathcal{O}_{K_{\mathfrak{p}}}[x]$$

and

$$d = \nu_\pi(f'_\pi(\pi)) = \nu_\pi(2\pi + a_1) = \min\{\nu_\pi(2\pi), \nu_\pi(a_1)\}.$$

Since $2\mathcal{O}_{K_{\mathfrak{p}}} = \mathcal{P}_{K_{\mathfrak{p}}}^{e_0}$ and $\mathcal{P}_{K_{\mathfrak{p}}}\mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{P}_{L_{\mathfrak{P}}}^2$, it follows that $2\mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{P}_{L_{\mathfrak{P}}}^{2e_0}$. Hence, $\nu_\pi(2) = 2e_0$ and $\nu_\pi(2\pi) = 2e_0 + 1$. Since $a_1 \in \mathcal{P}_{K_{\mathfrak{p}}}$, its valuation will be a multiple of 2. We now have

$$d = \min\{2e_0 + 1, \nu_\pi(a_1)\} \in \{2, 4, 6, \dots, 2e_0, 2e_0 + 1\}.$$

The form of f_π for each value of d is summarized in Table 3.1.

So f_π has the general form $f_\pi(x) = x^2 + \rho^k Ax + \rho B$ where $1 \le k \le e_0 + 1$. Note that the Newton-Ore exponents for this case are $c_1 = k$ and $c_2 = 1$. From Table 3.1, one observes that $k = \left\lfloor \frac{d+1}{2} \right\rfloor$.

According to Theorem 3.5, the coefficients of the characteristic polynomial for any $\beta \in \mathcal{P}_{L_{\mathfrak{P}}}$ will satisfy the same divisibility conditions as the coefficients of f_π. Next, any element $\beta \in \mathcal{O}_{L_{\mathfrak{P}}}$ is a translate by some $\gamma \in \Gamma$ of an element in $\mathcal{P}_{L_{\mathfrak{P}}}$. In particular,

$$\begin{aligned} f_{\mathfrak{P}}(x) &= (x+\gamma)^2 + \rho^k A(x+\gamma) + \rho B \\ &\equiv (x+\gamma)^2 + \rho B \pmod{\mathcal{P}_{K_{\mathfrak{p}}}^k} \end{aligned}$$

for some $A, B \in \mathcal{O}_{K_{\mathfrak{p}}}$ and some $\gamma \in \Gamma$.

The element $B \in \mathcal{O}_{K_{\mathfrak{p}}}$ can be written as a power series in ρ with coefficients from the set Γ:

$$B = b_0 + b_1\rho + b_2\rho^2 + \cdots \quad (b_i \in \Gamma).$$

Therefore,

$$f_{\mathfrak{P}}(x) \equiv (x+\gamma)^2 + \sum_{i=0}^{k-2} b_i \rho^{i+1} \pmod{\mathcal{P}_{K_{\mathfrak{p}}}^k}.$$

We summarize this result in the next theorem.

TABLE 3.1: The form of f_π for quadratic extensions.

d	Form of $f_\pi(x)$
2	$x^2 + \rho Ax + \rho B \quad (A, B \notin \mathcal{P}_{K_{\mathfrak{p}}})$
4	$x^2 + \rho^2 Ax + \rho B \quad (A, B \notin \mathcal{P}_{K_{\mathfrak{p}}})$
6	$x^2 + \rho^3 Ax + \rho B \quad (A, B \notin \mathcal{P}_{K_{\mathfrak{p}}})$
$\vdots$	$\vdots$
$2e_0$	$x^2 + \rho^{e_0} Ax + \rho B \quad (A, B \notin \mathcal{P}_{K_{\mathfrak{p}}})$
$2e_0 + 1$	$x^2 + \rho^{e_0+1} Ax + \rho B \quad (B \notin \mathcal{P}_{K_{\mathfrak{p}}})$

Theorem 3.6. *Let $e(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 2$, $f(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 1$, and suppose that $\mathcal{D}(L_\mathfrak{P}/K_\mathfrak{p}) = \mathcal{P}_{L_\mathfrak{P}}^d$. Then*

1. *$d \in \{2, 4, 6, \dots, 2e_0, 2e_0 + 1\}$, and*
2. *$f_\mathfrak{P}(x) \equiv (x+\gamma)^2 + \sum_{i=0}^{k-2} b_i \rho^{i+1} \pmod{\mathcal{P}_{K_\mathfrak{p}}^k}$ where $k = \lfloor \frac{d+1}{2} \rfloor$ and $\gamma, b_0, \dots, b_{k-2} \in \Gamma$. (when $k = 1$, there are no b_i's)*

3.3.2. Cubic Extensions. Here we assume $e = 3$ and $f = 1$. Also, for $L_\mathfrak{P}/K_\mathfrak{p}$ to be wildly ramified we must assume that $p = 3$.

For this case we have

$$f_\pi(x) = x^3 + a_1 x^2 + a_2 x + a_3 \in \mathcal{O}_{K_\mathfrak{p}}[x]$$

and

$$d = \nu_\pi(f_\pi'(\pi)) = \nu_\pi(3\pi^2 + 2a_1\pi + a_2) = \min\{\nu_\pi(3\pi^2), \nu_\pi(2a_1\pi), \nu_\pi(a_2)\}.$$

Since $3\mathcal{O}_{K_\mathfrak{p}} = \mathcal{P}_{K_\mathfrak{p}}^{e_0}$ and $\mathcal{P}_{K_\mathfrak{p}}\mathcal{O}_{L_\mathfrak{P}} = \mathcal{P}_{L_\mathfrak{P}}^3$, it follows that $3\mathcal{O}_{L_\mathfrak{P}} = \mathcal{P}_{L_\mathfrak{P}}^{3e_0}$. Hence, $\nu_\pi(3) = 3e_0$ and $\nu_\pi(3\pi^2) = 3e_0 + 2$. Since each $a_i \in \mathcal{P}_{K_\mathfrak{p}}$, their valuations will be a multiples of 3. Let $\nu_\pi(a_i) = 3k_i$. We now have

$$d = \min\{3e_0 + 2, 3k_1 + 1, 3k_2\} \in \{3, 4, 6, 7, 9, 10, \dots, 3e_0, 3e_0 + 1, 3e_0 + 2\}.$$

The form of f_π for each value of d is summarized in Table 3.2.

So f_π has the general form

$$f_\pi(x) = x^3 + \rho^{k_1} A x^2 + \rho^{k_2} B x + \rho C$$

where $1 \le k_i \le e_0 + 1$. Note that the Newton-Ore exponents for this case are $(k_1, k_2, 1)$. From Table 3.2, one observes that $k_1 = \lfloor \frac{d+1}{3} \rfloor$ and $k_2 = \lfloor \frac{d+2}{3} \rfloor$. We observe that $k_2 \ge k_1$, so the best congruences will be modulo $\mathcal{P}_{K_\mathfrak{p}}^{k_2}$.

TABLE 3.2: The form of f_π for cubic extensions.

d	Form of $f_\pi(x)$
3	$x^3 + \rho A x^2 + \rho B x + \rho C \quad (B, C \notin \mathcal{P}_{K_\mathfrak{p}})$
4	$x^3 + \rho A x^2 + \rho^2 B x + \rho C \quad (A, C \notin \mathcal{P}_{K_\mathfrak{p}})$
6	$x^3 + \rho^2 A x^2 + \rho^2 B x + \rho C \quad (B, C \notin \mathcal{P}_{K_\mathfrak{p}})$
7	$x^3 + \rho^2 A x^2 + \rho^3 B x + \rho C \quad (A, C \notin \mathcal{P}_{K_\mathfrak{p}})$
$\vdots$	$\vdots$
$3e_0$	$x^3 + \rho^{e_0} A x^2 + \rho^{e_0} B x + \rho C \quad (B, C \notin \mathcal{P}_{K_\mathfrak{p}})$
$3e_0 + 1$	$x^3 + \rho^{e_0} A x^2 + \rho^{e_0+1} B x + \rho C \quad (A, C \notin \mathcal{P}_{K_\mathfrak{p}})$
$3e_0 + 2$	$x^3 + \rho^{e_0+1} A x^2 + \rho^{e_0+1} B x + \rho C \quad (C \notin \mathcal{P}_{K_\mathfrak{p}})$

According to Theorem 3.5, the coefficients of the characteristic polynomial for any $\beta \in \mathcal{P}_{L_\mathfrak{P}}$ will satisfy the same divisibility conditions as the coefficients of f_π. Next, any element $\beta \in \mathcal{O}_{L_\mathfrak{P}}$ is a translate by some $\gamma \in \Gamma$ of an element in $\mathcal{P}_{L_\mathfrak{P}}$. In particular,

$$\begin{aligned} f_\mathfrak{P}(x) &= (x+\gamma)^3 + \rho^{k_1} A(x+\gamma)^2 + \rho^{k_2} B(x+\gamma) + \rho C \\ &\equiv (x+\gamma)^3 + \rho^{k_1} A(x+\gamma)^2 + \rho C \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_2}} \end{aligned}$$

for some $A, B, C \in \mathcal{O}_{K_\mathfrak{p}}$ and some $\gamma \in \Gamma$.

The elements A and C can each be written as a power series in ρ with coefficients from the set Γ:

$$A = a_0 + a_1\rho + a_2\rho^2 + \cdots \quad (a_i \in \Gamma).$$

$$C = c_0 + c_1\rho + c_2\rho^2 + \cdots \quad (c_i \in \Gamma).$$

Therefore,

$$f_\mathfrak{P}(x) \equiv (x+\gamma)^3 + \left(\sum_{i=0}^{k_2-k_1-1} a_i \rho^{k_1+i}\right)(x+\gamma)^2 + \sum_{i=0}^{k_2-2} c_i \rho^{i+1} \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_2}}.$$

We adopt the convention that when the lower limit of a summation exceeds the upper limit, then the sum is nonexistent. In summary, we have the following theorem.

Theorem 3.7. *Let $e(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 3$, $f(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 1$, and suppose that $\mathcal{D}(L_\mathfrak{P}/K_\mathfrak{p}) = \mathcal{P}_{L_\mathfrak{P}}^d$. Then $d \in \{3, 4, 6, 7, 9, 10, \ldots, 3e_0, 3e_0+1, 3e_0+2\}$, and*

$$f_\mathfrak{P}(x) \equiv (x+\gamma)^3 + \left(\sum_{i=0}^{k_2-k_1-1} a_i \rho^{k_1+i}\right)(x+\gamma)^2 + \sum_{i=0}^{k_2-2} c_i \rho^{i+1} \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_2}}$$

where $k_1 = \left\lfloor \frac{d+1}{3} \right\rfloor$, $k_2 = \left\lfloor \frac{d+2}{3} \right\rfloor$, and $\gamma, a_i, c_i \in \Gamma$.

Regarding Theorem 3.7, if $d \not\equiv 1 \pmod 3$ then $k_1 = k_2$ and all a_i's are zero. When $d \equiv 1 \pmod 3$, then $k_2 = k_1 + 1$ and the middle term reduces to $a_0\rho^{k_2-1}(x+\gamma)^2$.

3.3.3. Quartic Extensions with $f = 1$. Here we assume $e = 4$ and $f = 1$. Also, for $L_\mathfrak{P}/K_\mathfrak{p}$ to be wildly ramified we must assume that $p = 2$.

For this case we have

$$f_\pi(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in \mathcal{O}_{K_\mathfrak{p}}[x]$$

and

$$\begin{aligned} d = \nu_\pi(f_\pi'(\pi)) &= \nu_\pi(4\pi^3 + 3a_1\pi^2 + 2a_2\pi + a_3) \\ &= \min\{\nu_\pi(4\pi^3), \nu_\pi(3a_1\pi^2), \nu_\pi(2a_2\pi), \nu_\pi(a_3)\}. \end{aligned}$$

Since $2\mathcal{O}_{K_\mathfrak{p}} = \mathcal{P}_{K_\mathfrak{p}}^{e_0}$ and $\mathcal{P}_{K_\mathfrak{p}}\mathcal{O}_{L_\mathfrak{P}} = \mathcal{P}_{L_\mathfrak{P}}^4$, it follows that $2\mathcal{O}_{L_\mathfrak{P}} = \mathcal{P}_{L_\mathfrak{P}}^{4e_0}$. Hence, $\nu_\pi(2) = 4e_0$, $\nu_\pi(2\pi) = 4e_0 + 1$, and $\nu_\pi(4\pi^3) = 8e_0 + 3$. Since each $a_i \in \mathcal{P}_{K_\mathfrak{p}}$, their valuations will be multiples of 4. Let $\nu_\pi(a_i) = 4k_i$. We now have

$$\begin{aligned} d &= \min\{8e_0+3, 4k_1+2, 4k_2+4e_0+1, 4k_3\} \\ &\in \{4,6,8,\ldots,8e_0+2\} \cup \{4e_0+5, 4e_0+9, \ldots, 8e_0+1\} \cup \{8e_0+3\}. \end{aligned}$$

Since we are only interested in cases having $[L:\mathbb{Q}] \le 10$, we only need to consider $e_0 \le 2$. The form of f_π for these values of e_0 is summarized in Tables 3.3 and 3.4.

So f_π has the general form

$$f_\pi(x) = x^4 + \rho^{k_1}Ax^3 + \rho^{k_2}Bx^2 + \rho^{k_3}Cx + \rho D.$$

For this case, the Newton-Ore exponents are $(k_1, k_2, k_3, 1)$. Its not too hard to show that $k_1 = \lfloor \frac{d+1}{4} \rfloor$, $k_3 = \lfloor \frac{d+3}{4} \rfloor$, and

$$k_2 = \begin{cases} 1 & \text{if } d \le 4e_0 + 5 \\ \lfloor \frac{d+2}{4} \rfloor - e_0 & \text{if } d > 4e_0 + 5 \end{cases}$$

These expressions are valid for all e_0. Also, observe that $k_3 \ge k_i$ for all i, so the best congruences will be modulo $\mathcal{P}_{K_\mathfrak{p}}^{k_3}$.

According to Theorem 3.5, the coefficients of the characteristic polynomial for any $\beta \in \mathcal{P}_{L_\mathfrak{P}}$ will satisfy the same divisibility conditions as the coefficients of f_π. Next, any element $\beta \in \mathcal{O}_{L_\mathfrak{P}}$ is a translate by some $\gamma \in \Gamma$ of an element in $\mathcal{P}_{L_\mathfrak{P}}$. In particular,

$$\begin{aligned} f_\mathfrak{P}(x) &= (x+\gamma)^4 + \rho^{k_1}A(x+\gamma)^3 + \rho^{k_2}B(x+\gamma)^2 + \rho^{k_3}C(x+\gamma) + \rho D \\ &\equiv (x+\gamma)^4 + \rho^{k_1}A(x+\gamma)^3 + \rho^{k_2}B(x+\gamma)^2 + \rho D \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_3}} \end{aligned}$$

for some $A, B, C, D \in \mathcal{O}_{K_\mathfrak{p}}$ and some $\gamma \in \Gamma$.

The elements A, B, and D can each be written as a power series in ρ with coefficients from the set Γ:

$$A = a_0 + a_1\rho + a_2\rho^2 + \cdots \quad (a_i \in \Gamma).$$

Table 3.3: The form of f_π for quartic extensions when $e_0 = 1$.

d	Form of $f_\pi(x)$
4	$x^4 + \rho Ax^3 + \rho Bx^2 + \rho Cx + \rho D \quad (C, D \notin \mathcal{P}_{K_\mathfrak{p}})$
6	$x^4 + \rho Ax^3 + \rho Bx^2 + \rho^2 Cx + \rho D \quad (A, D \notin \mathcal{P}_{K_\mathfrak{p}})$
8	$x^4 + \rho^2 Ax^3 + \rho Bx^2 + \rho^2 Cx + \rho D \quad (C, D \notin \mathcal{P}_{K_\mathfrak{p}})$
9	$x^4 + \rho^2 Ax^3 + \rho Bx^2 + \rho^3 Cx + \rho D \quad (B, D \notin \mathcal{P}_{K_\mathfrak{p}})$
10	$x^4 + \rho^2 Ax^3 + \rho^2 Bx^2 + \rho^3 Cx + \rho D \quad (A, D \notin \mathcal{P}_{K_\mathfrak{p}})$
11	$x^4 + \rho^3 Ax^3 + \rho^2 Bx^2 + \rho^3 Cx + \rho D \quad (D \notin \mathcal{P}_{K_\mathfrak{p}})$

TABLE 3.4: The form of f_π for quartic extensions when $e_0 = 2$.

d	Form of $f_\pi(x)$	
4	$x^4 + \rho A x^3 + \rho B x^2 + \rho C x + \rho D$	$(C, D \notin \mathcal{P}_{K_\mathfrak{p}})$
6	$x^4 + \rho A x^3 + \rho B x^2 + \rho^2 C x + \rho D$	$(A, D \notin \mathcal{P}_{K_\mathfrak{p}})$
8	$x^4 + \rho^2 A x^3 + \rho B x^2 + \rho^2 C x + \rho D$	$(C, D \notin \mathcal{P}_{K_\mathfrak{p}})$
10	$x^4 + \rho^2 A x^3 + \rho B x^2 + \rho^3 C x + \rho D$	$(A, D \notin \mathcal{P}_{K_\mathfrak{p}})$
12	$x^4 + \rho^3 A x^3 + \rho B x^2 + \rho^3 C x + \rho D$	$(C, D \notin \mathcal{P}_{K_\mathfrak{p}})$
13	$x^4 + \rho^3 A x^3 + \rho B x^2 + \rho^4 C x + \rho D$	$(B, D \notin \mathcal{P}_{K_\mathfrak{p}})$
14	$x^4 + \rho^3 A x^3 + \rho^2 B x^2 + \rho^4 C x + \rho D$	$(A, D \notin \mathcal{P}_{K_\mathfrak{p}})$
16	$x^4 + \rho^4 A x^3 + \rho^2 B x^2 + \rho^4 C x + \rho D$	$(C, D \notin \mathcal{P}_{K_\mathfrak{p}})$
17	$x^4 + \rho^4 A x^3 + \rho^2 B x^2 + \rho^5 C x + \rho D$	$(B, D \notin \mathcal{P}_{K_\mathfrak{p}})$
18	$x^4 + \rho^4 A x^3 + \rho^3 B x^2 + \rho^5 C x + \rho D$	$(A, D \notin \mathcal{P}_{K_\mathfrak{p}})$
19	$x^4 + \rho^5 A x^3 + \rho^3 B x^2 + \rho^5 C x + \rho D$	$(D \notin \mathcal{P}_{K_\mathfrak{p}})$

$$B = b_0 + b_1\rho + b_2\rho^2 + \cdots \qquad (b_i \in \Gamma).$$
$$D = d_0 + d_1\rho + d_2\rho^2 + \cdots \qquad (d_i \in \Gamma).$$

Therefore,

$$\begin{aligned} f_\mathfrak{P}(x) \;\equiv\; & (x+\gamma)^4 + \left(\sum_{i=0}^{k_3-k_1-1} a_i \rho^{k_1+i}\right)(x+\gamma)^3 \\ & + \left(\sum_{i=0}^{k_3-k_2-1} b_i \rho^{k_2+i}\right)(x+\gamma)^2 + \sum_{i=0}^{k_3-2} d_i \rho^{i+1} \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_3}}. \end{aligned}$$

Again, we use the convention that when the lower limit of a summation exceeds the upper limit, then the sum is zero. In summary, we have the following theorem

Theorem 3.8. *Let $e(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 4$, $f(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 1$, and suppose that $\mathcal{D}(L_\mathfrak{P}/K_\mathfrak{p}) = \mathcal{P}_{L_\mathfrak{P}}^d$. Then*

$$d \in \{4, 6, 8, \ldots, 8e_0+2\} \cup \{4e_0+5, 4e_0+9, \ldots, 8e_0+1\} \cup \{8e_0+3\}$$

and

$$\begin{aligned} f_\mathfrak{P}(x) \;\equiv\; & (x+\gamma)^4 + \left(\sum_{i=0}^{k_3-k_1-1} a_i \rho^{k_1+i}\right)(x+\gamma)^3 \\ & + \left(\sum_{i=0}^{k_3-k_2-1} b_i \rho^{k_2+i}\right)(x+\gamma)^2 + \sum_{i=0}^{k_3-2} d_i \rho^{i+1} \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_3}} \end{aligned}$$

where $\gamma, a_i, b_i, d_i \in \Gamma$; $k_1 = \left\lfloor \frac{d+1}{4} \right\rfloor$, $k_3 = \left\lfloor \frac{d+3}{4} \right\rfloor$, and

$$k_2 = \begin{cases} 1 & \text{if } d \le 4e_0+5 \\ \left\lfloor \frac{d+2}{4} \right\rfloor - e_0 & \text{if } d > 4e_0+5 \end{cases}.$$

3.3.4. Quartic Extensions with $e = f = 2$. Here we assume $e = 2$ and $f = 2$. Also, for $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ to be wildly ramified we must assume that $p = 2$.

As in section 3.2.2, we let E be the intermediate field between $K_{\mathfrak{p}}$ and $L_{\mathfrak{P}}$ such that $L_{\mathfrak{P}}/E$ is totally ramified and $E/K_{\mathfrak{p}}$ is unramified. Also, we let $\hat{\Gamma} \subseteq \mathcal{O}_E$ be a complete set of representatives for $\mathcal{O}_E/\mathcal{P}_E$. Then $\hat{\Gamma}$ is also a complete set of representatives for $\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{P}_{L_{\mathfrak{P}}}$.

Since $[E : K_{\mathfrak{p}}] = f = 2$, there are 2 embeddings of E fixing $K_{\mathfrak{p}}$, which we denote $\sigma_1 = 1$ and σ_2. Since $E/K_{\mathfrak{p}}$ is necessarily Galois, $\sigma_2(E) = E$. We denote the conjugate for any $\beta \in E$ by $\beta^* = \sigma_2(\beta)$.

Since Theorem 3.5 only applies to totally ramified extensions, we must consider the minimal polynomial for π over E:

$$f_\pi(x) = x^2 + a_1 x + a_2 \in \mathcal{O}_E[x].$$

Recall that d represents the exponent of $\mathcal{P}_{L_{\mathfrak{P}}}$ in $\mathcal{D}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Since $E/K_{\mathfrak{p}}$ is unramified, d is also the exponent of $\mathcal{P}_{L_{\mathfrak{P}}}$ in $\mathcal{D}(L_{\mathfrak{P}}/E)$. Therefore,

$$d = \nu_\pi(f'_\pi(\pi)) = \nu_\pi(2\pi + a_1) = \min\{\nu_\pi(2\pi), \nu_\pi(a_1)\}.$$

As in the $f = 1$ case, we get $\nu_\pi(2\pi) = 2e_0 + 1$ and $\nu_\pi(a_1) = 2k$ for some $k \geq 1$. The possible values for d and the corresponding polynomial $f_\pi(x)$ are the same as they were in the $f = 1$ case, so Table 3.1 still applies. The only difference is that f_π is defined over $\mathcal{O}_E$ instead of $\mathcal{O}_{K_{\mathfrak{p}}}$, and we replace ρ with ρ_E, where ρ_E is a uniformizer for E. So f_π has the general form

$$f_\pi(x) = x^2 + \rho_E^k A x + \rho_E B$$

where $k = \left\lfloor \frac{d+1}{2} \right\rfloor$ and $A, B \in \mathcal{O}_E$.

According to Theorem 3.5, the coefficients of the characteristic polynomial for any $\beta \in \mathcal{P}_{L_{\mathfrak{P}}}$ will satisfy the same divisibility conditions as the coefficients of f_π; and, any element $\beta \in \mathcal{O}_{L_{\mathfrak{P}}}$ is a translate by some $\hat{\gamma} \in \hat{\Gamma}$ of an element in $\mathcal{P}_{L_{\mathfrak{P}}}$. In particular,

$$\begin{aligned} c_{\beta,E}(x) &= (x - \hat{\gamma})^2 + \rho_E^k A(x - \hat{\gamma}) + \rho_E B \\ &\equiv (x - \hat{\gamma})^2 + \rho_E B \pmod{\mathcal{P}_E^k} \end{aligned}$$

for some $A, B \in \mathcal{O}_E$ and some $\hat{\gamma} \in \hat{\Gamma}$. The characteristic polynomial for β^* is given by

$$\begin{aligned} c_{\beta^*,E}(x) &= \sigma_2(c_{\beta,E}(x)) \\ &\equiv (x - \hat{\gamma}^*)^2 + \rho_E^* B^* \pmod{\mathcal{P}_E^k}. \end{aligned}$$

Therefore, the characteristic polynomial over $K_{\mathfrak{p}}$ is

$$\begin{aligned} c_{\beta,K_{\mathfrak{p}}}(x) &\equiv \left[(x - \hat{\gamma})^2 + \rho_E B\right]\left[(x - \hat{\gamma}^*)^2 + \rho_E^* B^*\right] \pmod{\mathcal{P}_E^k} \\ &= [(x - \hat{\gamma})(x - \hat{\gamma}^*)]^2 + \rho_E B(x - \hat{\gamma}^*)^2 + \rho_E^* B^*(x - \hat{\gamma})^2 \\ &\quad + \rho_E \rho_E^* B B^* \\ &= [(x - \hat{\gamma})(x - \hat{\gamma}^*)]^2 + (\rho_E B + \rho_E^* B^*)x^2 - 2(\rho_E B \hat{\gamma}^* + \rho_E^* B^* \hat{\gamma})x \\ &\quad + \left(\rho_E B(\hat{\gamma}^*)^2 + \rho_E^* B^* \hat{\gamma}^2 + \rho_E \rho_E^* B B^*\right). \end{aligned} \tag{3.8}$$

Since all coefficients in Equation 3.8 are in $\mathcal{O}_{K_\mathfrak{p}}$, this congruence can be viewed modulo $\mathcal{P}_{K_\mathfrak{p}}^k$. Also, since $2\mathcal{O}_{K_\mathfrak{p}} = \mathcal{P}_{K_\mathfrak{p}}^{e_0}$, we observe that $2(\rho_E B\hat{\gamma}^* + \rho_E^* B^*\hat{\gamma}) \in \mathcal{P}_{K_\mathfrak{p}}^{e_0+1}$, and since $k \leq e_0 + 1$ this term is zero modulo $\mathcal{P}_{K_\mathfrak{p}}^k$. Similarly, one observes that the x^2 and constant terms are congruent to zero modulo $\mathcal{P}_{K_\mathfrak{p}}$. Putting all these ideas together, we may write

$$\begin{aligned} c_{\beta,K_\mathfrak{p}}(x) &\equiv [(x-\hat{\gamma})(x-\hat{\gamma}^*)]^2 + A'x^2 + B' \pmod{\mathcal{P}_{K_\mathfrak{p}}^k} \\ &= [(x^2 - (\hat{\gamma}+\hat{\gamma}^*)x + \hat{\gamma}\hat{\gamma}^*)]^2 + A'x^2 + B' \end{aligned} \tag{3.9}$$

where

$$A' = \begin{cases} 0 & \text{if } k = 1 \\ \displaystyle\sum_{i=0}^{k-2} a_i \rho^{i+1} & \text{if } k > 1 \end{cases} \tag{3.10}$$

$$B' = \begin{cases} 0 & \text{if } k = 1 \\ \displaystyle\sum_{i=0}^{k-2} b_i \rho^{i+1} & \text{if } k > 1 \end{cases} \tag{3.11}$$

and $a_i, b_i \in \Gamma$.

All we have left is to write $\hat{\gamma}$ in terms of elements from Γ. To do this, we first need an expression for $\hat{\Gamma}$ in terms of Γ.

Since $\mathcal{O}_E/\mathcal{P}_E \cong \mathbb{F}_{p^{2f_0}}$ is a quadratic extension of $\mathcal{O}_{K_\mathfrak{p}}/\mathcal{P}_{K_\mathfrak{p}} \cong \mathbb{F}_{p^{f_0}}$, and there is precisely one finite field (up to isomorphism) of order p^{2f_0}, any irreducible quadratic over $\mathbb{F}_{p^{f_0}}$ will generate $\mathbb{F}_{p^{2f_0}}$. So let $f_{\overline{\eta}}(x)$ be an irreducible quadratic over $\mathcal{O}_{K_\mathfrak{p}}/\mathcal{P}_{K_\mathfrak{p}}$ with root $\overline{\eta}$, say

$$f_{\overline{\eta}}(x) = x^2 + (d_1 + \mathcal{P}_{K_\mathfrak{p}})x + (d_0 + \mathcal{P}_{K_\mathfrak{p}})$$

where $d_0, d_1 \in \mathcal{O}_{K_\mathfrak{p}}$. Without loss of generality, we may assume $d_0, d_1 \in \Gamma$ (since Γ is a complete set of representatives for $\mathcal{O}_{K_\mathfrak{p}}/\mathcal{P}_{K_\mathfrak{p}}$). For example, when $f_0 = 1$, $\Gamma = \{0, 1\}$ and we may take $d_0 = d_1 = 1$ because $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$.

Now let η be any element of $\mathcal{O}_E$ such that $\overline{\eta} = \eta + \mathcal{P}_E$. Then $f_\eta(x) = x^2 + d_1x + d_0$ is irreducible over $\mathcal{O}_{K_\mathfrak{p}}$, because if it were reducible this would contradict the irreducibility of $f_{\overline{\eta}}$. It follows that $E = K_\mathfrak{p}(\eta)$.

Next, since $\mathcal{O}_E/\mathcal{P}_E = \mathcal{O}_{K_\mathfrak{p}}/\mathcal{P}_{K_\mathfrak{p}}(\overline{\eta})$, any $\overline{\lambda} \in \mathcal{O}_E/\mathcal{P}_E$ may be written $\overline{\lambda}_0 + \overline{\lambda}_1\overline{\eta}$ for some $\overline{\lambda}_0, \overline{\lambda}_1 \in \mathcal{O}_{K_\mathfrak{p}}/\mathcal{P}_{K_\mathfrak{p}}$. Then $\lambda_i \equiv \gamma_i$ modulo $\mathcal{P}_{K_\mathfrak{p}}$ for some $\gamma_i \in \Gamma$. So we may take

$$\hat{\Gamma} = \{\gamma_0 + \gamma_1\eta \mid \gamma_0, \gamma_1 \in \Gamma\} \tag{3.12}$$

as our complete set of representatives for $\mathcal{O}_E/\mathcal{P}_E$.

We now return to our analysis of Equation 3.9. First note that

$$f_\eta(x) = x^2 - (\eta + \eta^*)x + \eta\eta^* = x^2 + d_1x + d_0$$

so that $\eta + \eta^* = -d_1$ and $\eta\eta^* = d_0$. Now from Equation 3.12, we may write $\hat{\gamma} = \gamma_0 + \gamma_1\eta$ for some $\gamma_0, \gamma_1 \in \Gamma$. Therefore,

$$\hat{\gamma} + \hat{\gamma}^* = 2\gamma_0 + \gamma_1(\eta + \eta^*) = 2\gamma_0 - d_1\gamma_1$$

$$\begin{aligned}\hat{\gamma}\hat{\gamma}^* &= (\gamma_0 + \gamma_1\eta)(\gamma_0 + \gamma_1\eta^*) \\ &= \gamma_0^2 + \gamma_0\gamma_1(\eta + \eta^*) + \gamma_1^2\eta\eta^* \\ &= \gamma_0^2 - d_1\gamma_0\gamma_1 + d_0\gamma_1^2.\end{aligned}$$

We have proven the following theorem.

Theorem 3.9. *Let $e(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 2$, $f(\mathcal{P}_{L_\mathfrak{P}}/\mathcal{P}_{K_\mathfrak{p}}) = 2$, and suppose that $\mathcal{D}(L_\mathfrak{P}/K_\mathfrak{p}) = \mathcal{P}_{L_\mathfrak{P}}^d$. Furthermore, choose $d_0, d_1 \in \Gamma$ so that $x^2 + \overline{d}_1 x + \overline{d}_0$ is irreducible over $\mathcal{O}_K/\mathfrak{p}$. Then $d \in \{2, 4, 6, \ldots, 2e_0, 2e_0 + 1\}$, and*

$$\begin{aligned}f_\mathfrak{P}(x) \equiv\ & \left[x^2 + (2\gamma_0 - d_1\gamma_1)x + (\gamma_0^2 - d_1\gamma_0\gamma_1 + d_0\gamma_1^2)\right]^2 \\ & + A'x^2 + B' \pmod{\mathcal{P}_{K_\mathfrak{p}}^k}\end{aligned}$$

where $\gamma_0, \gamma_1 \in \Gamma$; A' and B' are given by Equations 3.10 and 3.11 respectively; and $k = \lfloor \frac{d+1}{2} \rfloor$.

3.3.5. Quintic Extensions. Here we assume $e = 5$ and $f = 1$. Also, for $L_\mathfrak{P}/K_\mathfrak{p}$ to be wildly ramified we must assume that $p = 5$.

For this case we have

$$f_\pi(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 \in \mathcal{O}_{K_\mathfrak{p}}[x]$$

and

$$\begin{aligned}d &= \nu_\pi(f'_\pi(\pi)) \\ &= \nu_\pi(5\pi^4 + 4a_1\pi^3 + 3a_2\pi^2 + 2a_3\pi + a_4) \\ &= \min\{\nu_\pi(5\pi^4), \nu_\pi(4a_1\pi^3), \nu_\pi(3a_2\pi^2), \nu_\pi(2a_3\pi), \nu_\pi(a_4)\}.\end{aligned}$$

Since $5\mathcal{O}_{K_\mathfrak{p}} = \mathcal{P}_{K_\mathfrak{p}}^{e_0}$ and $\mathcal{P}_{K_\mathfrak{p}}\mathcal{O}_{L_\mathfrak{P}} = \mathcal{P}_{L_\mathfrak{P}}^5$, it follows that $5\mathcal{O}_{L_\mathfrak{P}} = \mathcal{P}_{L_\mathfrak{P}}^{5e_0}$. Hence, $\nu_\pi(5) = 5e_0$ and $\nu_\pi(5\pi^4) = 5e_0 + 4$. Since each $a_i \in \mathcal{P}_{K_\mathfrak{p}}$, their valuations will be a multiples of 5. Let $\nu_\pi(a_i) = 5k_i$. We now have

$$\begin{aligned}d &= \min\{5e_0 + 4, 5k_1 + 3, 5k_2 + 2, 5k_3 + 1, 5k_4\} \\ &\in \{5, 6, 7, \ldots, 5e_0 + 4\} \backslash \{9, 14, \ldots, 5e_0 - 1\}.\end{aligned}$$

Since we are only interested in cases having $[L : \mathbb{Q}] \leq 10$, we only need to consider $e_0 \leq 2$. The form of f_π for these values of e_0 is summarized in Tables 3.5 and 3.6.

So f_π has the general form

$$f_\pi(x) = x^5 + \rho^{k_1}Ax^4 + \rho^{k_2}Bx^3 + \rho^{k_3}Cx^2 + \rho^{k_4}Dx + \rho E.$$

The corresponding Newton-Ore exponents are $(k_1, k_2, k_3, k_4, 1)$. One can easily show that $k_1 = \lfloor \frac{d+1}{5} \rfloor$, $k_2 = \lfloor \frac{d+2}{5} \rfloor$, $k_3 = \lfloor \frac{d+3}{5} \rfloor$, and $k_4 = \lfloor \frac{d+4}{5} \rfloor$. Observe that $k_4 \geq k_i$ for all i, so the best congruences will be modulo $\mathcal{P}_{K_\mathfrak{p}}^{k_4}$. Also note that $k_4 - k_i \in \{0, 1\}$ for each i.

TABLE 3.5: The form of f_π for quintic extensions when $e_0 = 1$.

d	Form of $f_\pi(x)$
5	$x^5 + \rho A x^4 + \rho B x^3 + \rho C x^2 + \rho D x + \rho E \quad (D, E \notin \mathcal{P}_{K_\mathfrak{p}})$
6	$x^5 + \rho A x^4 + \rho B x^3 + \rho C x^2 + \rho^2 D x + \rho E \quad (C, E \notin \mathcal{P}_{K_\mathfrak{p}})$
7	$x^5 + \rho A x^4 + \rho B x^3 + \rho^2 C x^2 + \rho^2 D x + \rho E \quad (B, E \notin \mathcal{P}_{K_\mathfrak{p}})$
8	$x^5 + \rho A x^4 + \rho^2 B x^3 + \rho^2 C x^2 + \rho^2 D x + \rho E \quad (A, E \notin \mathcal{P}_{K_\mathfrak{p}})$
9	$x^5 + \rho^2 A x^4 + \rho^2 B x^3 + \rho^2 C x^2 + \rho^2 D x + \rho E \quad (E \notin \mathcal{P}_{K_\mathfrak{p}})$

TABLE 3.6: The form of f_π for quintic extensions when $e_0 = 2$.

d	Form of $f_\pi(x)$
5	$x^5 + \rho A x^4 + \rho B x^3 + \rho C x^2 + \rho D x + \rho E \quad (D, E \notin \mathcal{P}_{K_\mathfrak{p}})$
6	$x^5 + \rho A x^4 + \rho B x^3 + \rho C x^2 + \rho^2 D x + \rho E \quad (C, E \notin \mathcal{P}_{K_\mathfrak{p}})$
7	$x^5 + \rho A x^4 + \rho B x^3 + \rho^2 C x^2 + \rho^2 D x + \rho E \quad (B, E \notin \mathcal{P}_{K_\mathfrak{p}})$
8	$x^5 + \rho A x^4 + \rho^2 B x^3 + \rho^2 C x^2 + \rho^2 D x + \rho E \quad (A, E \notin \mathcal{P}_{K_\mathfrak{p}})$
10	$x^5 + \rho^2 A x^4 + \rho^2 B x^3 + \rho^2 C x^2 + \rho^2 D x + \rho E \quad (D, E \notin \mathcal{P}_{K_\mathfrak{p}})$
11	$x^5 + \rho^2 A x^4 + \rho^2 B x^3 + \rho^2 C x^2 + \rho^3 D x + \rho E \quad (C, E \notin \mathcal{P}_{K_\mathfrak{p}})$
12	$x^5 + \rho^2 A x^4 + \rho^2 B x^3 + \rho^3 C x^2 + \rho^3 D x + \rho E \quad (B, E \notin \mathcal{P}_{K_\mathfrak{p}})$
13	$x^5 + \rho^2 A x^4 + \rho^3 B x^3 + \rho^3 C x^2 + \rho^3 D x + \rho E \quad (A, E \notin \mathcal{P}_{K_\mathfrak{p}})$
14	$x^5 + \rho^3 A x^4 + \rho^3 B x^3 + \rho^3 C x^2 + \rho^3 D x + \rho E \quad (E \notin \mathcal{P}_{K_\mathfrak{p}})$

According to Theorem 3.5, the coefficients of the characteristic polynomial for any $\beta \in \mathcal{P}_{L_\mathfrak{P}}$ will satisfy the same divisibility conditions as the coefficients of f_π. Next, any element $\beta \in \mathcal{O}_{L_\mathfrak{P}}$ is a translate by some $\gamma \in \Gamma$ of an element in $\mathcal{P}_{L_\mathfrak{P}}$. In particular,

$$\begin{aligned} f_\mathfrak{P}(x) &= (x+\gamma)^5 + \rho^{k_1} A (x+\gamma)^4 + \rho^{k_2} B (x+\gamma)^3 + \rho^{k_3} C (x+\gamma)^2 \\ &\quad + \rho^{k_4} E (x+\gamma) + \rho D \\ &\equiv (x+\gamma)^5 + \rho^{k_1} A (x+\gamma)^4 + \rho^{k_2} B (x+\gamma)^3 + \rho^{k_3} C (x+\gamma)^2 \\ &\quad + \rho D \pmod{\mathcal{P}_{K_\mathfrak{p}}^{k_4}} \end{aligned}$$

for some $A, B, C, D, E \in \mathcal{O}_{K_\mathfrak{p}}$ and some $\gamma \in \Gamma$.

The elements A, B, C, and D can each be written as a power series in ρ with coefficients from the set Γ:

$$A = a_0 + a_1 \rho + a_2 \rho^2 + \cdots \quad (a_i \in \Gamma).$$

$$B = b_0 + b_1 \rho + b_2 \rho^2 + \cdots \quad (b_i \in \Gamma).$$

$$C = c_0 + c_1 \rho + c_2 \rho^2 + \cdots \quad (c_i \in \Gamma).$$

$$D = d_0 + d_1 \rho + d_2 \rho^2 + \cdots \quad (d_i \in \Gamma).$$

Therefore,

$$f_{\mathfrak{P}}(x) \equiv (x+\gamma)^5 + A'(x+\gamma)^4 + B'(x+\gamma)^3 + C'(x+\gamma)^2 + D' \pmod{\mathcal{P}_{K_{\mathfrak{p}}}^{k_4}}$$

where

$$A' = \begin{cases} 0 & \text{if } k_1 = k_4 \\ a_0\rho^{k_1} & \text{if } k_1 = k_4 - 1 \end{cases} \tag{3.13}$$

$$B' = \begin{cases} 0 & \text{if } k_2 = k_4 \\ b_0\rho^{k_2} & \text{if } k_2 = k_4 - 1 \end{cases} \tag{3.14}$$

$$C' = \begin{cases} 0 & \text{if } k_3 = k_4 \\ c_0\rho^{k_3} & \text{if } k_3 = k_4 - 1 \end{cases} \tag{3.15}$$

$$D' = \begin{cases} 0 & \text{if } k_4 = 1 \\ \displaystyle\sum_{i=0}^{k_4-2} d_i\rho^{i+1} & \text{if } k_4 > 1 \end{cases} \tag{3.16}$$

We have proven the following theorem:

Theorem 3.10. *Let* $e(\mathcal{P}_{L_{\mathfrak{P}}}/\mathcal{P}_{K_{\mathfrak{p}}}) = 5$*,* $f(\mathcal{P}_{L_{\mathfrak{P}}}/\mathcal{P}_{K_{\mathfrak{p}}}) = 1$*, and suppose that* $\mathcal{D}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \mathcal{P}_{L_{\mathfrak{P}}}^d$*. Then*

$$d \in \{5, 6, 7, \ldots, 5e_0 + 4\} \backslash \{9, 14, \ldots, 5e_0 - 1\}$$

and

$$f_{\mathfrak{P}}(x) \equiv (x+\gamma)^5 + A'(x+\gamma)^4 + B'(x+\gamma)^3 + C'(x+\gamma)^2 + D' \pmod{\mathcal{P}_{K_{\mathfrak{p}}}^{k_4}}$$

where $\gamma \in \Gamma$*;* A'*,* B'*,* C'*, and* D' *are given by Equations 3.13, 3.14, 3.15, and 3.16 respectively; and for* $1 \leq i \leq 4$*,* $k_i = \left\lfloor \frac{d+i}{5} \right\rfloor$*.*

CHAPTER 4

PROOF OF THEOREM 3.5

The goal of this chapter is to provide a proof of Theorem 3.5, which we restate here for convenience:

Theorem 3.5. *Let L/K be a totally ramified extension of local fields. Then any $\alpha \in \mathcal{P}_L$ satisfies the Newton-Ore exponent condition.*

We will provide 2 proofs of this theorem.

4.1. The First Proof

The general idea of this proof is to consider $\alpha = \pi(a + \pi\beta)$ where π is a uniformizer for L, $\beta \in \mathcal{O}_L$ is fixed, and $a \in \mathcal{O}_K$. The coefficients of $c_\alpha(x)$ are polynomials in a. We let $g_i(x)$ denote the polynomial for the ith coefficient. If a is relatively prime to ρ (where ρ is a uniformizer for K), then α is a uniformizer for L, and hence α satisfies the Newton-Ore exponent condition. Given a sufficient number of elements a_k satisfying $(a_k, \rho) = 1$ and $(a_k - a_j, \rho) = 1$ (for $k \neq j$), one shows that the content of $g_i(x)$ contains the appropriate power of ρ, which proves the theorem. To ensure there are a sufficient number of elements a_k satisfying the above conditions, we form an unramified extension K' of K and then consider L'/K' where $L' = LK'$. We will now give the details of the proof.

Proof. Let $e = [L : K]$, let π be a uniformizer for L, and let ρ be a uniformizer for K. Fix $\beta \in \mathcal{O}_L$ and let $a \in \mathcal{O}_K$. Let $\alpha = \pi(a + \pi\beta)$ and let $c_{\alpha,K}(x)$ denote the characteristic polynomial for α over K. We need to show that α satisfies the Newton-Ore exponent condition.

The first step is to show that the coefficients of $c_{\alpha,K}(x)$ are polynomials in a. Since L/K is totally ramified, $\mathcal{O}_L = \mathcal{O}_K[\pi]$ and hence β is a polynomial in π, say $\beta = b(\pi)$ where $b \in \mathcal{O}_K[x]$. Consider the resultant

$$R_y(f_\pi(y), x - y(z + yb(y)) \stackrel{\text{def}}{=} r(z, x).$$

Since the resultant is the determinant of a Sylvester matrix, and the elements of this matrix are in $\mathcal{O}_K[z][x]$, it follows that $r(z,x) \in \mathcal{O}_K[z][x]$ (See [2], Section 3.3.2). Also,

$$\begin{aligned} r(a,x) &= R_y(f_\pi(y), x - y(a + yb(y))) \\ &= \prod_{i=1}^{e} [x - \pi_i(a + \pi_i b(\pi_i))] \\ &= \prod_{i=1}^{e} (x - \alpha_i) \\ &= c_{\alpha,K}(x), \end{aligned}$$

and therefore the coefficients of $c_{\alpha,K}(x)$ are polynomials in a.

Now let $f \in \mathbb{Z}^+$ be arbitrary (we will choose its value later) and let K' be the unique unramified extension of K of degree f. Let $L' = LK'$ be the compositum of L with K'. Observe that L'/L is unramified of degree f and L'/K' is totally ramified of degree e. The situation is depicted in Figure 4.1. Since L'/L is unramified, π is a uniformizer for L' and $L' = K'(\pi)$.

Since $L' = K'(\pi)$, the exact same resultant argument as above shows that

$$c_{\alpha,K'}(x) = r(a,x) = c_{\alpha,K}(x).$$

Therefore, it suffices to prove Theorem 3.5 for L'/K'. Note that we may now take a to be in $\mathcal{O}_{K'}$.

Based on what we showed above, we may write

$$c_{\alpha,K'}(x) = \sum_{i=0}^{e} g_i(a) x^{e-i}$$

where $g_i(x) \in \mathcal{O}_K[x]$. One may also show that $\deg(g_i) = i$. For example,

$$g_1(a) = \sum_{i=1}^{e} \alpha_i = a \sum_{i=1}^{e} \pi_i + \sum_{i=1}^{e} \pi_i^2 \beta_i$$

FIGURE 4.1: Field diagram for proof 1.

$$\begin{tikzcd} L' \arrow[dr, dash, "\text{unram}", "f"'] \arrow[dd, dash, "e", "\text{totally ramified}"'] & \\ & L \arrow[dd, dash, "\text{totally ramified}", "e"'] \\ K' \arrow[dr, dash, "f", "\text{unram}"'] & \\ & K \end{tikzcd}$$

and

$$\begin{aligned} g_2(a) &= \sum_{i<j} \alpha_i \alpha_j \\ &= \sum_{i<j} \pi_i(a+\pi_i\beta_i)\pi_j(a+\pi_j\beta_j) \\ &= a^2\left(\sum_{i<j}\pi_i\pi_j\right) + a\left(\sum_{i<j}\pi_i\pi_j(\pi_i\beta_i+\pi_j\beta_j)\right) + \sum_{i<j}\pi_i^2\pi_j^2\beta_i\beta_j. \end{aligned}$$

Note that $\mathcal{O}_{K'}/\mathcal{P}_{K'} \cong \mathbb{F}_{p^{f\cdot f_0}}$ where f_0 is the residue class degree for $K/\mathbb{Q}_p$. Let $n = p^{f\cdot f_0} - 1$ and let $a_1, \ldots, a_n \in \mathcal{O}_{K'}$ be representatives from the non-zero cosets of $\mathcal{P}_{K'}$ (*i.e.* $a_i \not\equiv a_j$ modulo $\mathcal{P}_{K'}$ for $i \neq j$). If $\rho \mid a_i$ then $a_i \in \rho\mathcal{O}_{K'} = \mathcal{P}_{K'}$, a contradiction. Therefore, each a_i is relatively prime to ρ.

Now consider $g_k(x)$ for $1 \leq k \leq e$, which we may write in the form:

$$g_k(x) = \gamma_k x^k + \gamma_{k-1}x^{k-1} + \cdots + \gamma_1 x + \gamma_0$$

where each $\gamma_i \in \mathcal{O}_K$. Since a_i is relatively prime to ρ, $\alpha = \pi(a_i + \pi\beta)$ is another uniformizer for L', and so the coefficients for $c_{\alpha,K'}(x)$ will satisfy the minimal divisibility conditions. In other words,

$$\rho^{c_k} \mid g_k(a_i) \qquad (1 \leq i \leq n) \tag{4.1}$$

where c_k denotes the Newton-Ore exponent for the kth coefficient. We need to show that $\rho^{c_k} \mid g_k(a)$ for every $a \in \mathcal{O}_{K'}$.

Since f was arbitrary, we can choose it so that $n \geq e+1 \geq k+1$. Equation 4.1 can be used to give the following $k+1$ equations, written in matrix form:

$$\begin{bmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^k \\ 1 & a_2 & a_2^2 & \cdots & a_2^k \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{k+1} & a_{k+1}^2 & \cdots & a_{k+1}^k \end{bmatrix} \begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_k \end{bmatrix} = \rho^{c_k} \begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_k \end{bmatrix}$$

for some $\lambda_0, \lambda_1, \ldots, \lambda_k \in \mathcal{O}_{K'}$. Then $\vec{\gamma} = \rho^{c_k} V^{-1}\vec{\lambda}$ where V is the Vandermonde matrix for $a_1, \ldots, a_{k+1}$. The denominator of V^{-1} will be

$$\det(V) = \prod_{i<j}(a_i - a_j)^2.$$

If $\rho \mid (a_i - a_j)$ $(i \neq j)$ then $a_i - a_j \in \rho\mathcal{O}_{K'} = \mathcal{P}_{K'}$, contradicting the fact that each a_i is in a distinct coset. Therefore, V^{-1} will have no factors of ρ in its denominator, and hence $\rho^{c_k} \mid \gamma_i$ for each i. It follows that $\rho^{c_k} \mid g_k(x)$, completing the proof. $\square$

4.2. The Second Proof

The second proof is more of a brute force method. The general idea is to use Waring's formula to give an equation relating the kth coefficient to the kth power sum and the previous coefficients. One then proceeds by applying valuations to this equation. Although the idea is simple in principle, it does require the development of some machinery.

The discussion is divided into 3 parts. The first part deals with some general purpose results which are applicable across many branches of mathematics. The second part derives some properties of the Newton-Ore exponents. Finally, the third part proves Theorem 3.5 by combining the results of the first two parts.

4.2.1. General Purpose Results. We start with Waring's formula. Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ with roots α_i, and define the power sums to be $s_k = \sum_i \alpha_i^k$.

Theorem 4.1 (Waring)**.** *Let $k \in \{1, 2, \ldots, n\}$ and define*

$$J_k = \left\{ (j_1, \ldots, j_k) \;\middle|\; \sum_{i=1}^{k} i j_i = k \textit{ and } j_i \geq 0 \;\; \forall i \right\}.$$

Then

$$s_k = \sum_{\vec{j} \in J_k} (-1)^{j_2+j_4+j_6+\cdots} \frac{\left(\sum_{i=1}^{k} j_i - 1\right)!\; k}{\prod_{i=1}^{k}(j_i!)} a_1^{j_1} a_2^{j_2} \cdots a_k^{j_k}.$$

A proof of Theorem 4.1 can be found in [11]. We will also need the following two variations of Theorem 4.1.

Theorem 4.2. *Let $k \in \{1, 2, \ldots, n\}$. Then*

$$s_k = (-1)^{k+1} k a_k + \sum_{\vec{j} \in J'_k} (\pm 1) \frac{\left(\sum_{i=1}^{k-1} j_i - 1\right)!\; k}{\prod_{i=1}^{k-1}(j_i!)} a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}$$

where $J'_k = J_k \backslash \{(0, \ldots, 0, 1)\}$.

Theorem 4.3. *Let $k \geq 1$ and define*

$$J''_k = \left\{ (j_1, \ldots, j_n) \;\middle|\; \sum_{i=1}^{n} i j_i = k \textit{ and } j_i \geq 0 \;\; \forall i \right\}.$$

Then

$$s_k = \sum_{\vec{j} \in J''_k} (-1)^{j_2+j_4+j_6+\cdots} \frac{(\sum_{i=1}^{n} j_i - 1)!\; k}{\prod_{i=1}^{n}(j_i!)} a_1^{j_1} a_2^{j_2} \cdots a_n^{j_n}.$$

Proof. When $k \leq n$ then $j_i = 0$ for $i > k$, so this result is the same as Theorem 4.1. So we may assume $k > n$. Consider the polynomial $g(x) = x^{k-n} f(x)$. Since $g(x)$ has the same roots as $f(x)$ but also has 0 as a root with multiplicity $k - n$, it follows that the power sums for g and f are identical. Also, the coefficients for g are $(a_1, \ldots, a_n, 0, \ldots, 0)$. Applying Theorem 4.1 to g gives the desired equation. □

The next result we will need is a generalization of the binomial theorem, called the multinomial theorem. We provide a proof for the convenience of the reader.

Theorem 4.4 (Multinomial Theorem)**.** *Let $k, n \geq 1$ and define*

$$J_{n,k} = \left\{ (j_1, \ldots, j_n) \;\middle|\; \sum_{i=1}^{n} j_i = k \text{ and } j_i \geq 0 \;\; \forall i \right\}.$$

For any $x_1, \ldots, x_n$ we have

$$(x_1 + x_2 + \cdots + x_n)^k = \sum_{\vec{j} \in J_{n,k}} \frac{k!}{\prod_{i=1}^{n} (j_i!)} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}.$$

Proof. This is easily proved using the binomial theorem and induction on n. It is trivially true when $n = 1$, and when $n = 2$ it reduces to the binomial theorem. Now let $n > 2$ and suppose it is true for $n - 1$. Using the binomial theorem, we get

$$\begin{aligned} (x_1 + x_2 + \cdots + x_n)^k &= [(x_1 + x_2 + \cdots + x_{n-1}) + x_n]^k \\ &= \sum_{j_n=0}^{k} \binom{k}{j_n} (x_1 + x_2 + \cdots + x_{n-1})^{k-j_n} x_n^{j_n}. \end{aligned} \tag{4.2}$$

Next, by the induction hypothesis,

$$(x_1 + x_2 + \cdots + x_{n-1})^{k-j_n} = \sum_{\vec{j} \in J_{n-1,k-j_n}} \frac{(k-j_n)!}{\prod_{i=1}^{n-1} (j_i!)} x_1^{j_1} x_2^{j_2} \cdots x_{n-1}^{j_{n-1}}.$$

When $\vec{j} = (j_1, \ldots, j_{n-1}) \in J_{n-1,k-j_n}$ we get $\sum_{i=1}^{n} j_i = k$, and therefore $\sum_{j_n=0}^{k} \sum_{\vec{j} \in J_{n-1,k-j_n}} = \sum_{\vec{j} \in J_{n,k}}$. Equation 4.2 then becomes

$$\begin{aligned} (x_1 + x_2 + \cdots + x_n)^k &= \sum_{j_n=0}^{k} \sum_{\vec{j} \in J_{n-1,k-j_n}} \binom{k}{j_n} \frac{(k-j_n)!}{\prod_{i=1}^{n-1} (j_i!)} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \\ &= \sum_{\vec{j} \in J_{n,k}} \frac{k!}{\prod_{i=1}^{n} (j_i!)} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}. \end{aligned}$$

□

The final results for this section are some identities related to valuations of factorials.

Lemma 4.5. *Let $p \in \mathbb{Z}$ be prime. If $i + j = k$ where $i, j \geq 0$ then*

$$\nu_p(k!) \geq \nu_p(i!) + \nu_p(j!).$$

Proof. We use induction on k. The result is clearly true when $k = 1$. Fix $k > 1$ and suppose the theorem is true for $k - 1$. Let $i, j \geq 0$ be arbitrary but such that $i + j = k$. If either i or j is zero then the result is trivial, so we may assume both are non-zero. Without loss of generality, suppose $\nu_p(i) \leq \nu_p(j)$. Then

$$\nu_p(k) \geq \min\{\nu_p(i), \nu_p(j)\} = \nu_p(i).$$

Writing $(i - 1) + j = k - 1$, the induction hypothesis gives

$$\nu_p((k-1)!) \geq \nu_p((i-1)!) + \nu_p(j!).$$

Finally,

$$\begin{aligned} \nu_p(k!) &= \nu_p(k) + \nu_p((k-1)!) \\ &\geq \nu_p(k) + \nu_p((i-1)!) + \nu_p(j!) \\ &= \nu_p(i!) + \nu_p(j!) + [\nu_p(k) - \nu_p(i)] \\ &\geq \nu_p(i!) + \nu_p(j!). \end{aligned}$$

□

Lemma 4.6. *Let $p \in \mathbb{Z}$ be prime. If $\sum_{i=1}^{n} j_i = k$ where each $j_i \geq 0$ then*

$$\nu_p(k!) \geq \sum_{i=1}^{n} \nu_p(j_i!).$$

Proof. This is easily proved by repeated use of Lemma 4.5:

$$\begin{aligned} \nu_p(k!) &\geq \nu_p(j_1!) + \nu_p((j_2 + \cdots + j_n)!) \\ &\geq \nu_p(j_1!) + \nu_p(j_2!) + \nu_p((j_3 + \cdots + j_n)!) \\ &\vdots \\ &\geq \sum_{i=1}^{n} \nu_p(j_i!). \end{aligned}$$

□

The next lemma is an improvement over Lemma 4.6. This lemma is not necessary for proving Theorem 3.5, but for the sake of completeness we include it. The proof is omitted, but is not hard.

Lemma 4.7. *Let $p \in \mathbb{Z}$ be prime. If $\sum_{i=1}^{n} j_i = k$ where each $j_i \geq 0$ then*

$$\nu_p(k!) \geq \sum_{i=1}^{n} \nu_p(j_i!) + \left(\nu_p(k) - \min_i\{\nu_p(j_i)\}\right).$$

4.2.2. Properties of the Newton-Ore Exponents. Let L/K be a finite extension of local fields. Also, we assume L/K is totally ramified with ramification index e. As usual, we let $\mathcal{O}_K, \mathcal{O}_L$ denote the rings of integers, and we let $\mathcal{P}_L, \mathcal{P}_K$ denote the unique maximal ideals.

Throughout this section and the next we will let $c_1, \ldots, c_e$ denote the Newton-Ore exponents. In this section we will derive some relationships between the c_i's.

Let π be a uniformizer for $\mathcal{O}_L$ and let ρ be a uniformizer for $\mathcal{O}_K$. Write the minimal polynomial for π as

$$f_\pi(x) = x^e + a_1 x^{e-1} + a_2 x^{e-2} + \cdots + a_{e-2}x^2 + a_{e-1}x + a_e$$

where each $a_i \in \mathcal{O}_K$. Let $d_i = \nu_\rho(a_i)$. Let D denote the exponent of $\mathcal{P}_L$ in $\mathcal{D}(L/K)$. As shown in section 3.3, $D = \min_{0 \le i \le e-1}\{D_i\}$ where

$$D_i = ed_i + e - (k+1) + e\nu_\rho(e-k).$$

We are now ready to state our first result.

Lemma 4.8. *If* $\min\limits_{0 \le i \le e-1}\{D_i\} = D_k$ *then*

$$c_k + \nu_\rho(e-k) \le \nu_\rho(e).$$

Proof. Since c_0 is defined to be 0, this is clearly true when $k = 0$. When $k \neq 0$, we have $D_k < D_0$ and therefore

$$ed_k + e - (k+1) + e\nu_\rho(e-k) < ed_0 + e - 1 + e\nu_\rho(e).$$

$$\implies \quad ed_k + e\nu_\rho(e-k) < k + e\nu_\rho(e)$$

$$\implies \quad d_k + \nu_\rho(e-k) < \frac{k}{e} + \nu_\rho(e) \le \nu_\rho(e)$$

Finally, Definition 3.4 implies that $c_k = d_k$, completing the proof. □

Lemma 4.9. *Let* $j > 0$. *If* $\nu_\rho(e-j) \ge \nu_\rho(e)$ *then* $\min\limits_{0 \le i \le e-1}\{D_i\} \neq D_j$ *and* $c_j = 1$.

Proof. From Lemma 4.8 we see that D_j cannot be the minimum. Suppose that D_k is the minimum. Then Lemma 4.8 gives $c_k + \nu_\rho(e-k) \le \nu_\rho(e) \le \nu_\rho(e-j)$. This implies that

$$c_k + \delta_{j>k} + \nu_\rho(e-k) - \nu_\rho(e-j) \le 1.$$

Definition 3.4 then gives $c_j = 1$. □

Theorem 4.10. *Let* $i, j \in \{1, 2, \ldots, e\}$ *and suppose* $c_j > 1$. *Then*

$$c_i + \nu_\rho(i) \ge c_j + \nu_\rho(j) - \delta_{i<j}.$$

Proof. This is clearly true when $i = j$, so it suffices to assume $i \neq j$. Suppose that D_k is the minimum ($0 \leq k \leq e-1$). Then Definition 3.4 gives us

$$c_j = c_k + \delta_{j>k} + \nu_\rho(e-k) - \nu_\rho(e-j) \tag{4.3}$$

$$c_i = \max\{c_k + \delta_{i>k} + \nu_\rho(e-k) - \nu_\rho(e-i), 1\} \tag{4.4}$$

If $\nu_\rho(e) \leq \nu_\rho(j)$ then $\nu_\rho(e-j) \geq \min\{\nu_\rho(e), \nu_\rho(j)\} = \nu_\rho(e)$. But then Lemma 4.9 gives $c_j = 1$, a contradiction. Therefore, we must have $\nu_\rho(j) < \nu_\rho(e)$.

We then have $\nu_\rho(e-j) = \min\{\nu_\rho(e), \nu_\rho(j)\} = \nu_\rho(j)$, and Equation 4.3 becomes

$$c_j + \nu_\rho(j) = c_k + \delta_{j>k} + \nu_\rho(e-k). \tag{4.5}$$

Next, if $\nu_\rho(e) \neq \nu_\rho(i)$ then $\nu_\rho(e-i) = \min\{\nu_\rho(e), \nu_\rho(i)\} \leq \nu_\rho(i)$. Therefore,

$$\begin{aligned} c_i + \nu_\rho(i) &\geq c_i + \nu_\rho(e-i) \\ &\geq c_k + \delta_{i>k} + \nu_\rho(e-k) && \text{(By Eqn. 4.4)} \\ &= c_j + \nu_\rho(j) - \delta_{j>k} + \delta_{i>k} && \text{(By Eqn. 4.5)} \\ &\geq c_j + \nu_\rho(j) - \delta_{i<j}. \end{aligned}$$

We have left to consider the case when $\nu_\rho(e) = \nu_\rho(i)$. Starting with Equation 4.5 we get

$$\begin{aligned} c_j + \nu_\rho(j) &= c_k + \nu_\rho(e-k) + \delta_{j>k} \\ &\leq \nu_\rho(e) + \delta_{j>k} && \text{(By Lemma 4.8)} \\ &= \nu_\rho(i) + \delta_{j>k} \\ &\leq c_i + \nu_\rho(i). \end{aligned}$$

This completes the proof of the theorem. □

The next corollary follows directly from Theorem 4.10.

Corollary 4.11. *Let $i, j \in \{1, 2, \ldots, e\}$ and suppose $c_i > 1$ and $c_j > 1$. If $i < j$ then*

$$c_i + \nu_\rho(i) = c_j + \nu_\rho(j) + \varepsilon$$

where $\varepsilon \in \{0, 1\}$.

4.2.3. Proof of Theorem 3.5. We will use the same setup from the last section. In particular, we have an extension L/K of local fields, ρ is a uniformizer for K, and $c_1, \ldots, c_e$ are the Newton-Ore exponents. In addition, we let e_0 denote the ramification index for $K/\mathbb{Q}_p$.

Theorem 4.12. *Let $k \in \{1, 2, \ldots, e\}$, let $m \geq 0$, and suppose $c_k > 1$. Let $j_1, \ldots, j_e \geq 0$ such that $\sum_{i=1}^{e} i j_i = k + m$. Then*

$$\nu_\rho(k+m) + \nu_\rho\left(\left(\sum_{i=1}^{e} j_i - 1\right)!\right) - \sum_{i=1}^{e} \nu_\rho(j_i!) + \sum_{i=1}^{e} j_i c_i \geq c_k + \nu_\rho(k).$$

Proof. Choose $i_0 \in \{1, 2, \dots, e\}$ so that $\nu_\rho(i_0 j_{i_0})$ is minimum. Then

$$\nu_\rho(k+m) = \nu_\rho\left(\sum_{i=1}^{e} i j_i\right) \geq \nu_\rho(i_0 j_{i_0}) = \nu_\rho(i_0) + \nu_\rho(j_{i_0}).$$

Now since $c_k > 1$, Theorem 4.10 gives us

$$c_{i_0} + \nu_\rho(i_0) \geq c_k + \nu_\rho(k) - \delta_{i_0<k}.$$

We will now use Lemma 4.6. Since $\nu_\rho(a) = e_0 \nu_p(a)$ for any $a \in \mathbb{Z}_p$, we can replace p with ρ in Lemma 4.6. Using this lemma, we have

$$\begin{aligned}
&\nu_\rho\left(\left(\sum_{i=1}^{e} j_i - 1\right)!\right) - \sum_{i=1}^{e} \nu_\rho(j_i!) \\
&\qquad = \nu_\rho\left(\left(\sum_{i=1}^{e} j_i - 1\right)!\right) - \left[\sum_{i \neq i_0} \nu_\rho(j_i!) + \nu_\rho((j_{i_0}-1)!)\right] - \nu_\rho(j_{i_0}) \\
&\qquad \geq -\nu_\rho(j_{i_0}).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\nu_\rho(k+m) + \nu_\rho\left(\left(\sum_{i=1}^{e} j_i - 1\right)!\right) - \sum_{i=1}^{e} \nu_\rho(j_i!) + \sum_{i=1}^{e} j_i c_i \\
&\qquad \geq \nu_\rho(k+m) - \nu_\rho(j_{i_0}) + \sum_{i=1}^{e} j_i c_i \\
&\qquad \geq \nu_\rho(i_0) + c_{i_0} + (j_{i_0}-1)c_{i_0} + \sum_{i \neq i_0} j_i c_i \\
&\qquad \geq c_k + \nu_\rho(k) + \left[-\delta_{i_0<k} + (j_{i_0}-1)c_{i_0} + \sum_{i \neq i_0} j_i c_i\right].
\end{aligned}$$

We will be finished if we can show that the term in brackets is non-negative. If $j_{i_0} > 1$ or if there is more than one non-zero j_i then this is obviously true. The only other possibility is when $j_{i_0} = 1$ and it is the only non-zero j_i. But in that case we have $i_0 = k + m \geq k$ so that $\delta_{i_0<k} = 0$. Therefore, the bracketed term is always non-negative. $\square$

Corollary 4.13. *Let $2 \leq k \leq e-1$ and let $j_1, \dots, j_{k-1} \geq 0$ such that $\sum_{i=1}^{k-1} i j_i = k$. If $c_k > 1$ then*

$$\nu_\rho\left(\left(\sum_{i=1}^{k-1} j_i - 1\right)!\right) - \sum_{i=1}^{k-1} \nu_\rho(j_i!) + \sum_{i=1}^{k-1} j_i c_i \geq c_k.$$

Proof. Follows easily from Theorem 4.12 by setting $m = 0$ and $j_k = j_{k+1} = \cdots = j_e = 0$. $\square$

Corollary 4.14. *Let $\pi \in \mathcal{P}_L$ be a uniformizer for L and let t_k denote the kth power sum for π. Let $k \in \{1, 2, \ldots, e\}$ and let $m \geq 0$. If $c_k > 1$ then*

$$\nu_\rho(t_{k+m}) \geq c_k + \nu_\rho(k).$$

Proof. Write the minimal polynomial for π as

$$f_\pi(x) = x^e + b_1 x^{e-1} + \cdots + b_{e-1}x + b_e.$$

Since π is a uniformizer, the coefficients of f_π satisfy $\nu_\rho(b_i) \geq c_i$. From Theorem 4.3 we get

$$t_{k+m} = \sum_{\vec{j} \in J''_{k+m}} (\pm 1) \frac{(\sum_{i=1}^{e} j_i - 1)!\, (k+m)}{\prod_{i=1}^{e}(j_i!)} b_1^{j_1} b_2^{j_2} \cdots b_e^{j_e}$$

where

$$J''_{k+m} = \left\{ (j_1, \ldots, j_e) \;\middle|\; \sum_{i=1}^{e} i j_i = k+m \text{ and } j_i \geq 0 \;\; \forall i \right\}.$$

Finally, from Theorem 4.12 we get

$$\begin{aligned} \nu_\rho(t_{k+m}) &\geq \min_{\vec{j} \in J''_{k+m}} \left\{ \nu_\rho(k+m) + \nu_\rho\left(\left(\sum_{i=1}^{e} j_i - 1\right)!\right) \right. \\ &\qquad \left. - \sum_{i=1}^{e} \nu_\rho(j_i!) + \sum_{i=1}^{e} j_i c_i \right\} \\ &\geq c_k + \nu_\rho(k). \end{aligned}$$

□

We now have everything we need to prove Theorem 3.5.

Theorem 3.5. *Let L/K be a totally ramified extension of local fields. Then any $\alpha \in \mathcal{P}_L$ satisfies the Newton-Ore exponent condition.*

Proof. Let $\pi \in \mathcal{P}_L$ be any uniformizer for L and let $t_k = \sum_{i=1}^{e} \pi_i^k$ be the kth power sum for π. Write the minimal polynomial for π as

$$f_\pi(x) = x^e + b_1 x^{e-1} + \cdots + b_{e-1}x + b_e$$

and note that $\nu_\rho(b_i) \geq c_i$, where the c_i's are the Newton-Ore exponents.

Write the characteristic polynomial for α as

$$c_\alpha(x) = x^e + a_1 x^{e-1} + \cdots + a_{e-1}x + a_e.$$

We need to show that $\nu_\rho(a_i) \geq c_i$.

Since $\mathcal{O}_L = \mathcal{O}_K[\pi]$, α will take the form

$$\alpha = d_1 \pi + d_2 \pi^2 + \cdots + d_e \pi^e$$

where each $d_i \in \mathcal{O}_K$. If $\rho \nmid d_1$ then α is another uniformizer, and hence $\nu_\rho(a_i) \geq c_i$. So we may assume that $\rho \mid d_1$. Since $\rho = \varepsilon\pi^e$ for some $\varepsilon \in \mathcal{O}_L^\times$, α can be put into the form

$$\alpha = d_2\pi^2 + \cdots + d_{e+1}\pi^{e+1}.$$

Let $s_k = \sum_{i=1}^e \alpha_i^k$ be the kth power sum for α. The first thing we will show is that $\nu_\rho(s_k) \geq c_k + \nu_\rho(k)$ whenever $c_k > 1$. Start with Theorem 4.4 where we take $n = e$ and $x_i = d_{i+1}\pi^{i+1}$

$$\begin{aligned} \alpha^k &= \sum_{\vec{j}\in J_{e,k}} \frac{k!}{\prod_{i=1}^e (j_i!)} (d_2\pi^2)^{j_1}(d_3\pi^3)^{j_2}\cdots(d_{e+1}\pi^{e+1})^{j_e} \\ &= \sum_{\vec{j}\in J_{e,k}} \frac{k!}{\prod_{i=1}^e (j_i!)} d'\pi^{2j_1+3j_2+\cdots+(e+1)j_e} \end{aligned}$$

where $d' \in \mathcal{O}_K$ and

$$J_{e,k} = \left\{ (j_1, \ldots, j_e) \;\middle|\; \sum_{i=1}^e j_i = k \text{ and } j_i \geq 0 \;\; \forall i \right\}.$$

It follows that

$$s_k = \sum_{\vec{j}\in J_{e,k}} \frac{k!}{\prod_{i=1}^e (j_i!)} d' t_{2j_1+3j_2+\cdots+(e+1)j_e}.$$

Define $m = \sum_{i=1}^e i j_i$ and note that for $\vec{j} \in J_{e,k}$ we get

$$2j_1 + 3j_2 + \cdots + (e+1)j_e = k + m.$$

Therefore, if $c_k > 1$ then

$$\begin{aligned} \nu_\rho(s_k) &\geq \min_{\vec{j}\in J_{e,k}} \left\{ \nu_\rho(k!) - \sum_{i=1}^e \nu_\rho(j_i!) + \nu_\rho(t_{k+m}) \right\} \\ &\geq c_k + \nu_\rho(k) \end{aligned} \tag{4.6}$$

where we have used Lemma 4.6 and Corollary 4.14. (Note that Lemma 4.6 is still valid when we replace p with ρ.)

Next, we use Theorem 4.2 to write a_k in terms of s_k and $a_1, \ldots, a_{k-1}$:

$$(-1)^{k+1} a_k = \frac{s_k}{k} + \sum_{\vec{j}\in J'_k} (\pm 1) \frac{\left(\sum_{i=1}^{k-1} j_i - 1\right)!}{\prod_{i=1}^{k-1}(j_i!)} a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}} \tag{4.7}$$

where

$$J'_k = \left\{ (j_1, \ldots, j_{k-1}) \;\middle|\; \sum_{i=1}^{k-1} i j_i = k \text{ and } j_i \geq 0 \;\; \forall i \right\}.$$

We will use induction on k to show that $\nu_\rho(a_k) \geq c_k$. Because $\alpha \in \mathcal{P}_L$, it follows that $\nu_\rho(a_i) \geq 1$ for every i, so when considering a_k it suffices to assume $c_k > 1$. When $k = 1$, $a_1 = s_1$ and we have $\nu_\rho(a_1) = \nu_\rho(s_1) \geq c_1$. Now let $k > 1$ and suppose $\nu_\rho(a_i) \geq c_i$ for $1 \leq i \leq k-1$. From Equation 4.7 we have

$$\begin{aligned} \nu_\rho(a_k) &\geq \min\left(\nu_\rho\left(\frac{s_k}{k}\right), \min_{\vec{j}\in J'_k}\left\{\nu_\rho\left(\left(\sum_{i=1}^{k-1} j_i - 1\right)!\right)\right.\right. \\ &\qquad\qquad\qquad\qquad \left.\left. - \sum_{i=1}^{k-1}\nu_\rho(j_i!) + \sum_{i=1}^{k-1} j_i c_i\right\}\right) \\ &\geq c_k \end{aligned}$$

where we have used Equation 4.6 and Corollary 4.13. This completes the proof. □

CHAPTER 5

THE ALGORITHM

In previous chapters, we have discussed how to get Archimedean bounds on the polynomial coefficients and how to compute a complete set of congruences that the coefficients must satisfy. This chapter will discuss how these concepts are utilized to form the algorithm.

In this chapter, we assume we are given a degree m number field K, and also a finite set of integral primes S. We are interested in finding all degree n extension fields L/K which are unramified outside of S.

5.1. Representatives for the Residue Field

In Chapter 3 it was assumed that we had a complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$, which we denoted Γ. It is worth mentioning how such a set can be constructed. The following theorem provides an answer. For a proof, see proposition 2.4.6 and Corollary 2.4.7 in [3].

Theorem 5.1. *Let $[K:\mathbb{Q}] = m$ and let $\omega_1, \ldots, \omega_m$ be an integral basis for K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ with $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = f$, and let $A = [a_{ij}]_{ij}$ be its Hermite normal form. Let D_p be the set of indices $i \in [1, m]$ such that $a_{ii} = p$. Then*

1. *$|D_p| = f$, and*
2. *$\overline{\omega_i} \in \mathcal{O}_K/\mathfrak{p}$ for $i \in D_p$ are $\mathbb{F}_p$-linearly independent.*

So if we let

$$\{\omega'_1, \omega'_2, \ldots, \omega'_f\} = \{\omega_i \mid i \in D_p\}$$

then we can take

$$\Gamma = \left\{ \sum_{i=1}^{f} b_i \omega'_i \;\middle|\; 0 \le b_i \le p-1 \right\} \tag{5.1}$$

as our complete set of representatives for $\mathcal{O}_K/\mathfrak{p}$.

5.2. Discriminant Calculations

Before Martinet's bound can be calculated, it is first necessary to compute the absolute discriminant $|d_L|$. The value of $|d_L|$ is determined from d_K and the ramification structure which is being targeted.

Let S_K be the set of prime ideals of $\mathcal{O}_K$ which lie above any prime in S. Fix a prime ideal $\mathfrak{p} \in S_K$ and let p be the prime below $\mathfrak{p}$. Suppose we are targeting the ramification structure $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ with residue degrees $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.

We are interested in determining that portion of $|d_L|$ which can be attributed to $\mathfrak{p}$. We will start by computing the different $\mathcal{D}(L/K)$. From Dedekind's theorem, we know that $\mathfrak{P}_i$ is ramified in $\mathcal{O}_L$ if and only if $\mathfrak{P}_i$ divides $\mathcal{D}(L/K)$. Therefore, $\mathcal{D}(L/K)$ has the form:

$$\mathcal{D}(L/K) = \left(\prod_{i=1}^{g} \mathfrak{P}_i^{r_i}\right) \cdot \mathfrak{a} \tag{5.2}$$

where $\mathfrak{a}$ is an ideal relatively prime to each $\mathfrak{P}_i$, and each $r_i \geq 0$. Note that $r_i \geq e_i - 1$ with equality if and only if $\mathfrak{P}_i$ is tamely ramified or unramified. In particular, $r_i = 0$ if and only if $\mathfrak{P}_i$ is unramified.

The relative discriminant ideal is

$$\begin{aligned} \mathfrak{d}_{L/K} &= \mathcal{N}_{L/K}(\mathcal{D}(L/K)) \\ &= \left(\prod_{i=1}^{g} \mathcal{N}_{L/K}(\mathfrak{P}_i^{r_i})\right) \cdot \mathcal{N}_{L/K}(\mathfrak{a}) \\ &= \left(\prod_{i=1}^{g} \mathfrak{p}^{f_i r_i}\right) \cdot \mathcal{N}_{L/K}(\mathfrak{a}) \\ &= \mathfrak{p}_i^{s} \mathcal{N}_{L/K}(\mathfrak{a}) \end{aligned}$$

where $s = \sum_{i=1}^{g} f_i r_i$. The absolute discriminant is then given by

$$\begin{aligned} |d_L| &= |d_K|^{[L:K]} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) \\ &= |d_K|^n \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}^s) \mathcal{N}_{L/\mathbb{Q}}(\mathfrak{a})) \\ &= |d_K|^n p^{f_0 s} \mathcal{N}_{L/\mathbb{Q}}(\mathfrak{a}) \end{aligned}$$

where $f_0 = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. Note that the term $\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{a})$ might have additional factors of p, but all these factors can be attributed to a prime ideal different from $\mathfrak{p}$. The factor of p in $|d_L|$ which corresponds solely to $\mathfrak{p}$ is $p^{f_0 s}$, and we denote this factor $d_{L,\mathfrak{p}}$:

$$d_{L,\mathfrak{p}} \stackrel{\text{def}}{=} p^{f_0 \sum_{i=1}^{g} r_i f_i}. \tag{5.3}$$

It is now easy to compute $|d_L|$ for a specific targeted search. Suppose we are interested in fields ramified at $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Then $|d_L|$ is given by

$$|d_L| = |d_K|^n \prod_{i=1}^{k} d_{L,\mathfrak{p}_i}$$

where each $d_{L,\mathfrak{p}_i}$ will depend on the targeted ramification structure for $\mathfrak{p}_i$. Note that to obtain all field extensions L/K, we must search over all possible combinations of ramification structures.

Example 5.1. *Suppose we are interested in decics containing a quadratic subfield. Then we have $[L : K] = 5$ and $[K : \mathbb{Q}] = 2$. Let us further suppose that $S = \{5\}$. There is only one possibility for K, namely $K = \mathbb{Q}(\sqrt{5})$. We have $5\mathcal{O}_K = \mathfrak{p}^2$, so $e_0 = 2$ and $f_0 = 1$.*

First consider the ramification structure $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^5$. The local form will be a quintic extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. We let d denote the exponent of $\mathfrak{P}$ in $\mathcal{D}(L/K)$, which is the same as the exponent of $\mathcal{P}_{L_{\mathfrak{P}}}$ in $\mathcal{D}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. As shown in section 3.3.5, d can take 1 of 9 values (see Table 3.6). For this ramification structure we have

$$d_{L,\mathfrak{p}} = 5^d,$$

and since $\mathfrak{p}$ is the only prime ideal, we have

$$|d_L| = |d_K|^5 d_{L,\mathfrak{p}} = 5^{5+d}.$$

Now consider the ramification structure $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^3\mathfrak{P}_2^2$. This time ramification is tame and we have $e_1 = 3$, $e_2 = 2$, and $f_1 = f_2 = 1$. Therefore,

$$d_{L,\mathfrak{p}} = 5^{(e_1-1)f_1+(e_2-1)f_2} = 5^3,$$

and hence $|d_L| = |d_K|^5 d_{L,\mathfrak{p}} = 5^8$.

Now consider the ramification structure $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^2\mathfrak{P}_2$ where $f_1 = 2$ and $f_2 = 1$. Since ramification is tame, we get

$$d_{L,\mathfrak{p}} = 5^{(e_1-1)f_1} = 5^2,$$

and hence $|d_L| = |d_K|^5 d_{L,\mathfrak{p}} = 5^7$.

The other ramification structures are handled in a similar way.

5.3. Implementing the Bounds

Let $\sigma_1, \ldots, \sigma_m$ be the embeddings of K and let $\omega_1, \ldots, \omega_m$ be an integral basis for K. All of the archimedean bounds derived in Chapter 2 take the form

$$\vec{a}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{a} \leq B \tag{5.4}$$

where $Q = [\sigma_i(\omega_j)]_{ij}$, B is a positive real-valued bound, and $\vec{a}$ is either a polynomial coefficient or a power sum. The vector $\vec{a} = [a_1 \ldots a_m] \in \mathbb{Z}^m$ represents the element $a = \sum_{i=1}^m a_i\omega_i$.

The first issue we consider is how to convert the bound given by Equation 5.4 into separate bounds on each component a_i. Let $Q' = Q^{\mathrm{H}}Q$. Since $\vec{a}$ has real valued components, $\vec{a}^{\mathrm{T}}Q'\vec{a}$ is also real valued, and therefore

$$\vec{a}^{\mathrm{T}}Q'\vec{a} = \mathrm{Re}\{\vec{a}^{\mathrm{T}}Q'\vec{a}\} = \vec{a}^{\mathrm{T}}A\vec{a}$$

where $A = [\mathrm{Re}\{q'_{ij}\}]_{ij}$. Equation 5.4 then becomes

$$\vec{a}^{\mathrm{T}} A \vec{a} \leq B \tag{5.5}$$

Since $\vec{z}^{\mathrm{T}} A \vec{z} > 0$ for every non-zero $\vec{z} \in \mathbb{R}^m$, A is a positive definite symmetric real matrix, hence must have real positive eigenvalues. The eigenvector/eigenvalue decomposition of the matrix A is given by

$$A = E \Lambda E^{\mathrm{T}}$$

where E is the matrix whose columns are the eigenvectors of A and $\Lambda = \mathrm{diag}(\lambda_1, \ldots, \lambda_m)$ is the diagonal matrix of eigenvalues.

The cross product terms in Equation 5.5 are removed by considering the transformation $\vec{z} = E^{\mathrm{T}} \vec{a}$. This gives

$$\vec{z}^{\mathrm{T}} \Lambda \vec{z} = \vec{a}^{\mathrm{T}} E \Lambda E^{\mathrm{T}} \vec{a} = \vec{a}^{\mathrm{T}} A \vec{a} \leq B.$$

$$\implies \quad \lambda_1 z_1^2 + \lambda_2 z_2^2 + \cdots + \lambda_m z_m^2 \leq B. \tag{5.6}$$

Since each $\lambda_i > 0$, this region is the interior of an m-dimensional ellipsoid. It follows that $\vec{a}$ lies inside a rotated m-dimensional ellipsoid. For this reason, we will sometimes refer to bounds of the type given in Equation 5.5 as *ellipsoidal bounds*.

It is easy to use Equation 5.6 to get bounds on the z_i's, but this does not help to get bounds on the a_i's. To get good bounds on the a_i's, we start by forming a triangular decomposition for the matrix A. This is sometimes called the Cholesky decomposition. The existence of such a decomposition is provided by the following theorem, whose proof can be found in [6] (p. 114, 407).

Theorem 5.2. *A matrix A is positive definite if and only if there exists a non-singular upper triangular matrix T with positive diagonal entries such that $A = T^{\mathrm{T}} T$. If A is real then T is real. Furthermore, this triangular decomposition is unique.*

So we may decompose A uniquely as

$$A = T^{\mathrm{T}} T$$

where T is an upper triangular matrix with positive diagonal entries. Defining $\vec{z} = T\vec{a}$ we have

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1m} \\ 0 & t_{22} & \cdots & t_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t_{mm} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}$$

which implies

$$z_1^2 + z_2^2 + \cdots + z_m^2 = \vec{z}^{\mathrm{T}} \vec{z} = \vec{a}^{\mathrm{T}} T^{\mathrm{T}} T \vec{a} \leq B. \tag{5.7}$$

Substituting for z_i in Equation 5.7 we get

$$\left(\sum_{i=1}^{m} t_{1i}a_i\right)^2 + \left(\sum_{i=2}^{m} t_{2i}a_i\right)^2 + \cdots + (t_{mm}a_m)^2 \leq B.$$

This gives the following bound on a_m:

$$|a_m| \leq \frac{1}{t_{mm}} \cdot \sqrt{B}, \tag{5.8}$$

Given the value for a_m, we then derive the following bound on a_{m-1}:

$$|t_{m-1,m-1}a_{m-1} + t_{m-1,m}a_m| \leq \sqrt{B - (t_{mm}a_m)^2} \stackrel{\text{def}}{=} B_{m-1}. \tag{5.9}$$

$$\Longrightarrow \quad \frac{-B_{m-1} - t_{m-1,m}a_m}{t_{m-1,m-1}} \leq a_{m-1} \leq \frac{B_{m-1} - t_{m-1,m}a_m}{t_{m-1,m-1}}. \tag{5.10}$$

And in general, the bounds on a_j are computed from the current values of $a_{j+1}, \ldots, a_m$ as follows:

$$\frac{1}{t_{jj}}\left(-B_j - \sum_{k=j+1}^{m} t_{jk}a_k\right) \leq a_j \leq \frac{1}{t_{jj}}\left(B_j - \sum_{k=j+1}^{m} t_{jk}a_k\right) \tag{5.11}$$

where we define

$$B_j \stackrel{\text{def}}{=} \sqrt{B - \sum_{k=j+1}^{m}\left(\sum_{i=k}^{m} t_{ki}a_i\right)^2}. \tag{5.12}$$

We end this section with an explicit formula for the Cholesky decomposition. These formulas are derived by forming the product $T^{\mathrm{T}}T$ and equating it to $A = [a_{ij}]_{ij}$.

$$t_{11} = \sqrt{a_{11}}, \qquad t_{12} = \tfrac{a_{12}}{t_{11}}, \qquad t_{13} = \tfrac{a_{13}}{t_{11}}, \quad \cdots, \quad t_{1k} = \tfrac{a_{1k}}{t_{11}} \ .$$

$$t_{22} = \sqrt{a_{22} - t_{12}^2}, \qquad t_{23} = \tfrac{a_{23} - t_{12}t_{13}}{t_{22}}, \quad \cdots, \quad t_{2k} = \tfrac{a_{2k} - t_{12}t_{1k}}{t_{22}} \ .$$

$$t_{33} = \sqrt{a_{33} - t_{13}^2 - t_{23}^2}, \qquad t_{3k} = \tfrac{a_{3k} - t_{13}t_{1k} - t_{23}t_{2k}}{t_{33}} \ \ (k > 3) \ .$$

$$t_{44} = \sqrt{a_{44} - t_{14}^2 - t_{24}^2 - t_{34}^2}, \qquad t_{4k} = \tfrac{a_{4k} - t_{14}t_{1k} - t_{24}t_{2k} - t_{34}t_{3k}}{t_{44}} \ \ (k > 4) \ .$$

And in general,

$$t_{jj} = \sqrt{a_{jj} - \textstyle\sum_{i=1}^{j-1} t_{ij}^2}, \qquad t_{jk} = \tfrac{a_{jk} - \sum_{i=1}^{j-1} t_{ij}t_{ik}}{t_{jj}} \ \ (k > j). \tag{5.13}$$

As an example, when $m = 2$ the above equations give

$$T = \begin{bmatrix} \sqrt{a_{11}} & \frac{a_{12}}{\sqrt{a_{11}}} \\ 0 & \left(a_{22} - \frac{a_{12}^2}{a_{11}}\right)^{1/2} \end{bmatrix}.$$

5.4. Implementing the Congruences

In the previous section, we showed how to obtain bounds on the individual components of a coefficient $\vec{a}$ given a bound on $\vec{a}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{a}$. This method can be used directly when performing a standard Martinet search, but must be modified slightly in order to use the congruences on $\vec{a}$.

Suppose we want to find elements $a = \sum_{i=1}^{m} a_i \omega_i \in \mathcal{O}_K$ which are congruent to $c = \sum_{i=1}^{m} c_i \omega_i \in \mathcal{O}_K$ modulo the ideal $\mathfrak{a}$. The ideal $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank $m = [K : \mathbb{Q}]$, so there exist $\mu_j \in \mathcal{O}_K$ such that

$$\mathfrak{a} = \mu_1 \mathbb{Z} + \mu_2 \mathbb{Z} + \cdots + \mu_m \mathbb{Z}.$$

Each μ_j may be written $\mu_j = \sum_{i=1}^{m} \mu_{ij} \omega_i$ where $\mu_{ij} \in \mathbb{Z}$. Now if $a \equiv c \pmod{\mathfrak{a}}$ then $a - c \in \mathfrak{a}$ which implies

$$\begin{aligned} \sum_{i=1}^{m} a_i \omega_i - \sum_{i=1}^{m} c_i \omega_i &= k_1 \mu_1 + \cdots + k_m \mu_m \\ &= k_1 \sum_{i=1}^{m} \mu_{i1} \omega_i + \cdots + k_m \sum_{i=1}^{m} \mu_{im} \omega_i \end{aligned}$$

for some $k_i \in \mathbb{Z}$. Equating the coefficients of the ω_i's, we get the following matrix equation:

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} \mu_{11} & \mu_{12} & \cdots & \mu_{1m} \\ \mu_{21} & \mu_{22} & \cdots & \mu_{2m} \\ \vdots & \vdots & & \vdots \\ \mu_{m1} & \mu_{m2} & \cdots & \mu_{mm} \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ \vdots \\ k_m \end{bmatrix} + \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{bmatrix}$$

which we write as

$$\vec{a} = M \vec{k} + \vec{c}.$$

Note that there exists a basis for $\mathfrak{a}$ such that M will be in Hermite normal form. We will always assume that M is the Hermite normal form.

Now define $\vec{k}' = \vec{k} + M^{-1} \vec{c}$. Then

$$\vec{a} = M(\vec{k} + M^{-1} \vec{c}) = M \vec{k}'.$$

We now use the bound on $\vec{a}$ to give bounds on the k_i's. From Equation 5.4 we get

$$(\vec{k}')^{\mathrm{T}} (QM)^{\mathrm{H}} (QM) \vec{k}' \leq B.$$

As in section 5.3, there exists an auxiliary matrix A such that $(\vec{k}')^{\mathrm{T}} A \vec{k}' \leq B$ and A is a positive definite real symmetric matrix. Using the Cholesky decomposition for A as was done in section 5.3, we obtain the following bounds for the components of $\vec{k}'$.

$$|k'_m| \leq \frac{1}{t_{mm}} \cdot \sqrt{B}$$

$$\frac{-B_{m-1} - t_{m-1,m}k'_m}{t_{m-1,m-1}} \le k'_{m-1} \le \frac{B_{m-1} - t_{m-1,m}k'_m}{t_{m-1,m-1}}$$

$$\vdots$$

$$\frac{1}{t_{jj}}\left(-B_j - \sum_{i=j+1}^{m} t_{ji}k'_i\right) \le k'_j \le \frac{1}{t_{jj}}\left(B_j - \sum_{i=j+1}^{m} t_{ji}k'_i\right)$$

where

$$B_j \stackrel{\text{def}}{=} \sqrt{B - \sum_{r=j+1}^{m}\left(\sum_{i=r}^{m} t_{ri}k'_i\right)^2}.$$

If we write these bounds as $L'_i \le k'_i \le U'_i$, then we get the following bounds on the k_i's

$$\lceil L'_i - c'_i \rceil \le k_i \le \lfloor U'_i - c'_i \rfloor$$

where $\vec{c}\,' = M^{-1}\vec{c}$. We will write these bounds as $L_i \le k_i \le U_i$. Note that the bounds L_i and U_i depend on the current values of $k_{i+1}, \ldots, k_m$. So to obtain all values for $\vec{k}$, we first loop over the range for k_m. The current value for k_m is used to get looping bounds for k_{m-1}. Then the current values for k_m and k_{m-1} are used to get looping bounds for k_{m-2}, and so on.

The search algorithm works by looping over all combinations of the k_i's, and for each combination, computing $\vec{a} = M\vec{k} + \vec{c}$. Observe that the bounds on the k_i's are smaller than the bounds on the a_i's so that the search region has been reduced. What is happening here is easily understood by considering the one dimensional case, where we want all elements a such that $a = c + kp$ (here $\mu_1 = p$ is the modulus of the congruence vector). If the archimedean bounds are $|a| < B$ then $k = \frac{a-c}{p}$ so that $\frac{-B-c}{p} \le k \le \frac{B-c}{p}$. We see that the search region has been reduced by a factor of p, and as k loops over all integer values, a will loop over the multiples of p. The multi-dimensional case is completely analogous.

The above method must be modified slightly when the bound is on a power sum instead of a polynomial coefficient. Suppose we are interested in the jth ($2 \le j \le n-1$) polynomial coefficient and we have the following bound on the jth power sum:

$$\vec{s_j}^{\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_j} \le B.$$

From Newton's formulas, we may write

$$j\vec{a_j} = \vec{b_j} - \vec{s_j}$$

where $\vec{b_j} \in \mathbb{Z}^m$ depends on the coefficients $a_1, \ldots, a_{j-1}$. As usual, $\vec{b_j}$ is the vector representation for an element $b_j \in \mathcal{O}_K$. The first 3 values for b_j are

$$b_2 = a_1^2,$$

$$b_3 = -a_1^3 + 3a_1a_2,$$

and

$$b_4 = a_1^4 + 4a_1a_3 - 4a_1^2a_2 + 2a_2^2.$$

For this to work properly, we must assume that the looping order on the coefficients is $a_1, a_n, a_2, a_3, \ldots, a_{n-1}$. The reason a_n comes second is that it is needed in order to use the method of Pohst which gives the bounds on the power sums.

The coefficient $\vec{a_j}$ is still related to the congruence via the equation

$$\vec{a_j} = M\vec{k} + \vec{c}.$$

This time we define

$$\vec{c}\,' = \frac{1}{j}M^{-1}(\vec{b_j} - j\vec{c})$$

and

$$\vec{k}' = \vec{c}\,' - \vec{k}.$$

With these definitions, we may now write

$$\begin{aligned} \vec{s_j} &= \vec{b_j} - j\vec{a_j} \\ &= \vec{b_j} - j(M\vec{k} + \vec{c}) \\ &= jM\left[\frac{1}{j}M^{-1}(\vec{b_j} - j\vec{c}) - \vec{k}\right] \\ &= jM\vec{k}'. \end{aligned}$$

We now use the bound on $\vec{s_j}$ to give bounds on the components of $\vec{k}'$:

$$\vec{s_j}^{\,\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_j} = j^2 (\vec{k}')^{\mathrm{T}} (QM)^{\mathrm{H}} (QM) \vec{k}'.$$

$$\Longrightarrow \quad (\vec{k}')^{\mathrm{T}} (QM)^{\mathrm{H}} (QM) \vec{k}' = \frac{1}{j^2} \vec{s_j}^{\,\mathrm{T}} Q^{\mathrm{H}} Q \vec{s_j} \le \frac{B}{j^2}.$$

As in section 5.3, there exists an auxiliary matrix A such that $(\vec{k}')^{\mathrm{T}} A \vec{k}' \le \frac{B}{j^2}$ and A is a positive definite real symmetric matrix.

The rest of the algorithm is basically the same as before. The only difference is we use $\frac{B}{j^2}$ for the bound, and $k_j' = c_j' - k_j$.

5.5. Algorithm Summary

We now have everything we need to construct the algorithm. First we discuss the targeted Martinet search algorithm, and then we discuss the general algorithm for finding all extensions L/K which are unramified outside of S.

5.5.1. The Targeted Martinet Search. The input to the targeted Martinet search will be a vector of congruence data:

$$\vec{v} = [d_{L,\mathfrak{m}}, \mathfrak{m}, \vec{c_1}, \ldots, \vec{c_N}]$$

where $\mathfrak{m}$ is the modulus ideal for the congruences, $d_{L,\mathfrak{m}}$ is the portion of $|d_L|$ which can be attributed to the primes dividing $\mathfrak{m}$, N is the number of congruence vectors, and each $\vec{c_i}$ is a vector of congruences. Note that each $\vec{c_i}$ is of length $n = [L : K]$ where the jth component is the congruence for the jth coefficient. The algorithm is as follows:

1. If M is the Hermite normal form for $\mathfrak{m}$, then compute the t_{ij}'s corresponding to $Q' = (QM)^{\mathrm{H}}(QM)$ according to Equation 5.13. Note this will first require computing the auxiliary matrix $A = \left[\mathrm{Re}\{q'_{ij}\}\right]_{ij}$.
2. Compute $|d_L| = |d_K|^n \cdot d_{L,\mathfrak{m}}$.
3. Loop over congruence vectors $\vec{c_i} = [c_{i1}, \ldots, c_{in}]$.
4. Set $a_1 = c_{i1}$. Here it is assumed that the congruence vectors are constructed in such a way that the first congruence gives the first coefficient directly.
5. Compute Martinet's bound:
$$C_{a_1} = \frac{1}{n}\sum_{j=1}^{m} |\sigma_j(a_1)|^2 + \gamma_{m(n-1)} \left(\frac{|d_L|}{n^m|d_K|}\right)^{1/m(n-1)}.$$
6. Loop over the coefficient a_n where the bounds on a_n are computed according to Theorem 2.2, and the looping structure for the components of a_n is described in Section 5.4 above.
7. Use the method of Pohst (Theorem 2.7) to give bounds on s_3, s_4, …, s_{n-1}.
8. Loop over the rest of the coefficients in the order a_2, a_3, …, a_{n-1} as described in Section 5.4 above. For each combination of coefficients, do the following:
   (a) Form the polynomial
   $$f_{\alpha,K}(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n.$$
   (b) Compute the polynomial $f_L(x) \in \mathbb{Z}[x]$ representing the field $L = K(\alpha)$. In the pari/gp system, this can be done by using the function "rnfequation()".
   (c) Only continue if $\deg(f_L) = nm$. This is always true when n is prime, in which case this step can be skipped.
   (d) Compute the polynomial discriminant for f_L and divide out all factors of $p \in S$. Only continue if the result is a non-zero square.

(e) Only continue if f_L is irreducible.

(f) Finally, write f_L to file if the field discriminant of f_L divides $|d_L|$.

One may also incorporate the constraints of Section 2.4 by testing each coefficient inside of its respective looping structure.

5.5.2. Algorithm for Constructing Field Tables. The algorithm for finding all primitive degree n extensions L/K which are unramified outside of the set S is as follows.

1. Compute the set S_K of all prime ideals of $\mathcal{O}_K$ which lie above some $p \in S$.

2. For each $\mathfrak{p} \in S_K$, compute the complete set of congruence vector data $C_\mathfrak{p}$ according to the theorems of Chapter 3. This will entail computing Γ for each $\mathfrak{p}$ according to Equation 5.1. The elements of $C_\mathfrak{p}$ are vectors of the form

$$\vec{v} = [d_{L,\mathfrak{p}}, \mathfrak{p}^k, \vec{c_1}, \ldots, \vec{c_N}]$$

   where $\mathfrak{p}^k$ is the modulus ideal for the congruences, $d_{L,\mathfrak{p}}$ is the portion of $|d_L|$ which can be attributed to $\mathfrak{p}$, N is the number of congruence vectors, and each $\vec{c_i}$ is a vector of congruences.

3. Perform a standard Martinet search to find all primitive extensions L such that L/K is unramified.

4. For each $\mathfrak{p} \in S_K$, do a targeted Martinet search as described in Section 5.5.1 to find all primitive extensions L/K which are ramified at only $\mathfrak{p}$.

5. When $|S_K| \geq 2$, for each pair of primes $\mathfrak{p}, \mathfrak{q} \in S_K$, do a targeted search to find all primitive extensions L/K which are ramified at precisely $\mathfrak{p}$ and $\mathfrak{q}$. Before the search can be performed, the congruence data for $\mathfrak{p}$ and $\mathfrak{q}$ must be combined. The combined discriminant bound is $d_{L,\mathfrak{pq}} = d_{L,\mathfrak{p}} d_{L,\mathfrak{q}}$ and is that part of d_L which can be attributed to both $\mathfrak{p}$ and $\mathfrak{q}$. The combined modulus ideal is the product of the individual modulus ideals. Finally, the individual congruence vectors are combined in pairs using the Chinese remainder theorem for ideals. Note that a combined congruence vector can be discarded if the first congruence is not congruent to one of the allowed values for a_1 as dictated by Theorem 2.1.

6. When $|S_K| \geq 3$, for each triplet $\mathfrak{p}_i, \mathfrak{p}_j, \mathfrak{p}_k \in S_K$, do a targeted search to find all primitive extensions L/K which are ramified at precisely $\mathfrak{p}_i$, $\mathfrak{p}_j$, and $\mathfrak{p}_k$. The congruences are combined in a similar way to that described in step 5.

7. When $|S_K| \geq 4$, do a similar thing for all combinations of 4 prime ideals.

8. Continue in this manner until a targeted search has been performed to find all primitive extensions L/K which are ramified at precisely every prime ideal of S_K.

9. Refine the final list of polynomials to remove isomorphic fields.

To construct complete tables of imprimitive number fields of degree N which are unramified outside of the set S, the above algorithm is applied to every field K of degree m dividing N ($1 < m < N$), where K is also unramified outside of S. In this way, tables are built up inductively from tables of smaller degree fields.

CHAPTER 6

APPLICATIONS

The targeted Martinet search algorithm has multiple applications, which are now discussed.

6.1. The Calegari Conjecture

The following question was posted on a number theory e-mailing list by Frank Calegari:

> "I'm trying to show that there is no A_5 extension K of $\mathbb{Q}(i)$ with the following property:
> 1. $K/\mathbb{Q}(i)$ is unramified outside $(1+i)$, $(2+i)$, and $(2-i)$;
> 2. The discriminant of $K/\mathbb{Q}(i)$ divides the following number:
> $(1+i)^{48}(2+i)^{69}(2-i)^{117}$.
> Is this a plausible computation?"

The first step is to recast this question into a form more amenable to the targeted Martinet search algorithm.

Let $K = \mathbb{Q}(i)$ and let L be a degree $n = 5$ extension of K. Note that $2\mathcal{O}_K = \mathfrak{p}_1^2$ where $\mathfrak{p}_1 = (1+i)\mathcal{O}_K$, and $5\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_3$ where $\mathfrak{p}_2 = (2+i)\mathcal{O}_K$ and $\mathfrak{p}_3 = (2-i)\mathcal{O}_K$. Using our notation we have

$$S = \{2, 5\} \quad \text{and} \quad S_K = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}.$$

So Calegari's question is referring to quintic extensions of K which are unramified outside of S and which have Galois group A_5 over K.

Next, we will consider Calegari's discriminant condition. Calegari's discriminant bound applies to the Galois closure L^g of $L/\mathbb{Q}$, and can be stated as follows

$$\mathfrak{d}_{L^g/K} = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\mathfrak{p}_3^{n_3}$$

where $n_1 \le 48$, $n_2 \le 69$, and $n_3 \le 117$. Next, we will compute $|d_{L^g}|$. Observing that $[L^g : K] = |A_5| = 60$ we get

$$|d_{L^g}| = |d_K|^{60}\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}_{L^g/K}) = 4^{60}2^{n_1}5^{n_2}5^{n_3} = 2^{120+n_1}5^{n_2+n_3}.$$

Now suppose $|d_L| = 2^{m_1}5^{m_2}$. We wish to determine bounds on m_1 and m_2. Since $[L^g : L] = [L^g : K]/[L : K] = 60/5 = 12$, we get

$$|d_{L^g}| = |d_L|^{12}\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{d}_{L^g/L}),$$

and therefore

$$2^{120+n_1}5^{n_2+n_3} = 2^{12m_1}5^{12m_2}\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{d}_{L^g/L}),$$

which implies

$$12m_1 \leq 120 + n_1 \leq 168 \quad \text{and} \quad 12m_2 \leq n_2 + n_3 \leq 186.$$

Hence $m_1 \leq 14$ and $m_2 \leq 15$. So for Calegari's question to be true, it suffices to prove the following conjecture, which we will refer to as Calegari's Conjecture.

Conjecture 6.1. *There is no quintic extension L of $\mathbb{Q}(i)$ satisfying*

1. $\mathrm{Gal}(L^g/\mathbb{Q}(i)) = A_5$*,*
2. *L is unramified outside of $S = \{2, 5\}$, and*
3. *d_L divides $2^{14}5^{15}$.*

Let $G = \mathrm{Gal}(L^g/\mathbb{Q})$. Since 120 divides $|G|$ and L contains a quadratic subfield, one sees that

$$G \in \{T11, T12, T22, T40, T41, T42, T43\} \tag{6.1}$$

where we use the naming convention for the transitive groups as established in [1]. Analyzing each group in Equation 6.1 separately, it's not too hard to show the following:

Theorem 6.2. *Let K be a quadratic number field and let L be a quintic extension of K such that $\mathrm{Gal}(L^g/K) = A_5$. Then*

$$G \in \{T11, T12, T40\}.$$

We now have everything we need to apply the targeted Martinet search. Doing a complete search for the case when $K = \mathbb{Q}(i)$ and $S = \{2, 5\}$ turns out to be impractical. However, it is possible to do a search for all fields having $\nu_2(d_L) \leq 2^{17}$ (the maximum possible is 2^{29}) within a timely manner, and this is sufficient to cover Calegari's discriminant condition. After about a week of non-stop processing, the search yielded 104 non-isomorphic fields of which there were none of type T11, 1 of type T12, and 1 of type T40. The T12 and T40 polynomials are:

$$f_{T12} = x^{10} - 10x^7 + 45x^6 - 46x^5 + 50x^4 - 120x^3 + 100x^2 + 40x + 8,$$

$$f_{T40} = x^{10} - 2x^9 + 5x^8 - 12x^7 + 12x^6 - 20x^5 + 28x^4 + 20x^3 + 53x^2 + 42x + 9.$$

The T12 had discriminant $2^{12}5^{16}$ and the T40 had discriminant $2^{22}5^8$, both of which exceed Calegari's bound. This proves the truth of Calegari's Conjecture.

6.2. Verification of Old Tables

In [7], Jones and Roberts determine all sextic fields unramified outside the set $S = \{2, 3\}$. They used a targeted Hunter search which is only guaranteed to find the primitive sextics, and then they used class field theory to show that the list of discovered fields actually contained every sextic. On his web site [9], John Jones has additional tables of sextics with prescribed ramification; however, these tables were never proven complete. Performing targeted Martinet searches for all cases on this web site, it was proven that the tables are indeed complete.

6.3. Construction of New Tables

The most obvious application of the targeted Martinet search is to construct complete tables of imprimitive number fields. This was done for quartics, sextics, octics, nonics, and decics. Results for all cases except quartics are tabulated in Appendix A, and can also be found at either [9] or [10].

The biggest concern when using complex algorithms such as the targeted Martinet search, is the possibility of subtle programming errors, which may lead to erroneous results. In our case, a mistake usually leads to a missed field, and hence incomplete number field tables. In this section we discuss a method for checking the completeness of the tables.

Fix the set of primes S and let $G = xTy$ represent a Galois group of type Ty for a field of degree x. Then we let N_G be the number of fields with Galois group G which are unramified outside of S. In addition, we let N_{C_2}, N_{C_3}, and N_{S_3} be the number of quadratic, C_3 cubics, and S_3 cubics respectively.

The method for checking our field data involves analyzing each type of Galois group in order to count the number of expected fields of a given type as a function of the numbers of smaller degree fields. As an example, looking at the subgroup lattice for a $C_6 = 6T1$ sextic, we see that the C_6 sextic is the compositum of a quadratic with a C_3 cubic. Hence,

$$N_{6T1} = N_{C_2} N_{C_3}.$$

The method gives a series of tests which can be applied to the data in the tables to see if the numbers of certain types of fields are correct. It is important to note that the set of tests is not guaranteed to find all possible flaws in the data, but does allow us to say with a high degree of confidence that the data is complete.

We now list the various tests as a sequence of theorems, one theorem per degree. The proofs are omitted, but are not difficult.

Theorem 6.3 (Sextics)**.**

$$\begin{array}{ll} N_{6T1} = N_{C_2} N_{C_3} & N_{6T6} = N_{4T4} N_{C_2} \\ N_{6T2} = N_{S_3} & N_{6T7} = N_{4T5} \\ N_{6T3} = N_{S_3}(N_{C_2} - 1) & N_{6T8} = N_{4T5} \\ N_{6T4} = N_{4T4} & N_{6T11} = N_{4T5}(N_{C_2} - 1) \\ N_{6T5} = N_{C_3} N_{S_3} & \end{array}$$

Theorem 6.4 (Octics).

$$N_{8T2} = \tfrac{1}{4} N_{4T1}(N_{C_2} - 1)$$
$$N_{8T3} = \tfrac{1}{28} N_{4T2}(N_{C_2} - 3)$$
$$N_{8T4} = \tfrac{1}{2} N_{4T3}$$
$$N_{8T6} \equiv 0 \pmod 2$$
$$N_{8T9} = \tfrac{1}{4} N_{4T3}(N_{C_2} - 3)$$
$$N_{8T10} \equiv 0 \pmod 2$$
$$N_{8T11} \equiv 0 \pmod 3$$
$$N_{8T13} = N_{4T4} N_{C_2}$$
$$N_{8T14} = N_{4T5}$$
$$N_{8T15} \equiv 0 \pmod 2$$
$$N_{8T16} \equiv 0 \pmod 2$$
$$N_{8T17} \equiv 0 \pmod 2$$
$$N_{8T18} \equiv 0 \pmod 8$$
$$N_{8T19} = 2N_{8T20}$$
$$N_{8T20} = N_{8T21}$$
$$N_{8T22} \equiv 0 \pmod 6$$
$$N_{8T23} \equiv 0 \pmod 2$$
$$N_{8T24} = N_{4T5}(N_{C_2} - 1)$$
$$N_{8T26} \equiv 0 \pmod 4$$
$$N_{8T27} \equiv 0 \pmod 2$$
$$N_{8T28} = N_{8T27}$$
$$N_{8T29} = 3N_{8T31}$$
$$N_{8T30} \equiv 0 \pmod 4$$
$$N_{8T31} \equiv 0 \pmod 2$$
$$N_{8T32} \equiv 0 \pmod 3$$
$$N_{8T33} \equiv 0 \pmod 2$$
$$N_{8T35} \equiv 0 \pmod 8$$
$$N_{8T38} \equiv 0 \pmod 2$$
$$N_{8T39} \equiv 0 \pmod 6$$
$$N_{8T40} \equiv 0 \pmod 2$$
$$N_{8T41} \equiv 0 \pmod 2$$
$$N_{8T44} \equiv 0 \pmod 4$$

Theorem 6.5 (Nonics).

$$N_{9T2} = \tfrac{1}{12} N_{C_3}(N_{C_3} - 1)$$
$$N_{9T4} = N_{C_3} N_{S_3}$$
$$N_{9T5} = \tfrac{1}{6}[\tfrac{1}{2} N_{S_3}(N_{S_3} - 1) - N_{6T9}]$$
$$N_{9T7} \equiv 0 \pmod 4$$
$$N_{9T8} = N_{6T9}$$
$$N_{9T11} = N_{9T13}$$
$$N_{9T12} \equiv 0 \pmod 4$$
$$N_{9T17} \equiv 0 \pmod 3$$
$$N_{9T18} \equiv 0 \pmod 2$$
$$N_{9T20} \equiv 0 \pmod 3$$
$$N_{9T21} \equiv 0 \pmod 3$$
$$N_{9T22} \equiv 0 \pmod 3$$
$$N_{9T24} \equiv 0 \pmod 3$$

Theorem 6.6 (Decics).

$$N_{10T1} = N_{C_2} N_{5T1}$$
$$N_{10T2} = N_{5T2}$$
$$N_{10T3} = N_{5T2}(N_{C_2} - 1)$$
$$N_{10T4} = N_{5T3}$$
$$N_{10T5} = N_{5T3}(N_{C_2} - 1)$$
$$N_{10T6} = 2N_{5T1} N_{5T2}$$
$$N_{10T8} \equiv 0 \pmod 3$$
$$N_{10T9} = 2N_{5T2}(N_{5T2} - 1)$$
$$N_{10T10} \equiv 0 \pmod 2$$
$$N_{10T11} = N_{C_2} N_{5T4}$$
$$N_{10T12} = N_{5T5}$$
$$N_{10T14} \equiv 0 \pmod 3$$
$$N_{10T15} \equiv 0 \pmod 3$$
$$N_{10T16} = N_{10T15}$$
$$N_{10T17} \equiv 0 \pmod 2$$
$$N_{10T18} \equiv 0 \pmod 3$$
$$N_{10T20} \equiv 0 \pmod 3$$
$$N_{10T21} = 2N_{10T19}$$
$$N_{10T22} = N_{5T5}(N_{C_2} - 1)$$
$$N_{10T23} \equiv 0 \pmod 6$$
$$N_{10T23} > 0 \implies N_{10T15} \geq 3$$
$$N_{10T24} = N_{10T25}$$
$$N_{10T27} \equiv 0 \pmod 3$$
$$N_{10T29} \equiv 0 \pmod 2$$
$$N_{10T29} > 0 \implies N_{10T24} > 0$$
$$N_{10T37} = N_{10T38}$$
$$N_{10T39} \equiv 0 \pmod 2$$
$$N_{10T39} > 0 \implies N_{10T37} > 0$$

REFERENCES

[1] Gregory Butler and John McKay, The transitive groups of degree up to 11, Comm. Algebra 11 (1983), 863-911.

[2] Henri Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, New York, 1996.

[3] Henri Cohen, Advanced Topics in Computational Number Theory, Springer-Verlag, New York, 2000.

[4] F. Diaz Y Diaz and M. Olivier, Imprimitive ninth-degree number fields with small discriminants, Math. Comp. 64 (1995), 305-321.

[5] C. Hermite, Sur le nombre limité d'irrationalités auxquelle se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés (Extrait d'une lettre à M. Borchardt), J. Reine Angew. Math. 53, (1857), 182-192 = Oeuvres, I, Paris 1905 414-428.

[6] Roger A. Horn and Charles R. Johnson, Matrix Analysis, Cambridge University Press, Cambridge, 1985.

[7] J. Jones and D. Roberts, Sextic number fields with discriminant $(-1)^j 2^a 3^b$, in Number Theory: Fifth Conference of the Canadian Number Theory Association, CRM Proceedings and Lecture Notes, 19, American Math. Soc., (1999), 141-172.

[8] J. Jones and D. Roberts, Septic number fields with discriminant $\pm 2^a 3^b$, Math. Comp. 72 (2003), 1975-1985.

[9] J. Jones, Tables of number fields with prescribed ramification, `http://math.la.asu.edu/~jj/numberfields`

[10] E. Driver, Tables of number fields with prescribed ramification, `http://mathpost.la.asu.edu/~driver/`

[11] P. A. MacMahon, Combinatory analysis, Chelsea Publishing Co., New York, 1960.

[12] J. Martinet, Méthodes géométriques dans la recherche des petits discriminants, Prog. Math. 59, Birkhäuser, Boston (1985), 147-179.

[13] Ö. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, Math. Ann. 99 (1928), 84-117.

[14] M. Pohst, On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields, J. Number Theory 14 (1982), 99-117.

APPENDIX A

Tables of Fields with Prescribed Ramification

In this appendix, we provide complete tables of number fields unramified outside of a finite set of primes S. The tables give the numbers of each type of field and the total number of fields. There are tables for degrees 6, 8, 9 and 10. This information can also be found on the web, along with links to the data files [10].

A.1. Imprimitive Sextic Tables

In the following tables we use the naming convention of Butler and McKay [1]. In particular, we have

$$\begin{aligned} T_5 &= C_3^2 \rtimes C_2 & \qquad T_{10} &= C_3^2 \rtimes C_4 \\ T_6 &= A_4 \times C_2 & \qquad T_{11} &= S_4 \times C_2 \\ T_9 &= C_3^2 \rtimes C_2^2 & \qquad T_{13} &= C_3^2 \rtimes D_4. \end{aligned}$$

Table A.1: Imprimitive sextics where S contains 1 prime.

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{2}													0
{3}								1			1	1	3
{5}													0
{7}												1	1
{11}													0
{13}												1	1
{17}													0
{19}												1	1
{23}											1		1
{29}													0
{31}								1			1	1	3
{37}												1	1
{41}													0
{43}												1	1
{47}													0

continued on next page

Table A.1: Imprimitive sextics with $|S| = 1$ (*cont.*)

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
$\{53\}$													0
$\{59\}$					1	1					1		3
$\{61\}$												1	1
$\{67\}$												1	1
$\{71\}$													0
$\{73\}$												1	1
$\{79\}$												1	1
$\{83\}$											1		1
$\{89\}$													0
$\{97\}$												1	1
$\{101\}$													0
$\{103\}$												1	1
$\{107\}$					1	1					1		3
$\{109\}$												1	1
$\{113\}$													0
$\{127\}$												1	1
$\{131\}$													0
$\{137\}$													0
$\{139\}$					1	1		1			1	1	5
$\{149\}$			2										2
$\{151\}$												1	1
$\{157\}$												1	1
$\{163\}$							1		1			1	3
$\{167\}$													0
$\{173\}$													0
$\{179\}$													0
$\{181\}$												1	1
$\{191\}$													0
$\{193\}$												1	1
$\{197\}$													0
$\{199\}$								1			1	1	3
$\{211\}$								1			1	1	3
$\{223\}$												1	1
$\{227\}$													0
$\{229\}$					3	3		1			1	1	9

Table A.2: Imprimitive sextics where S contains 2 primes.

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{2,3}	50	132	4	22	22	22	7	8	1	48	8	7	331
{2,5}		18			3	3				6	1		31
{3,5}		2	2	4	1	1		5		10	5	3	33
{2,7}	2		2				7		1			7	19
{3,7}	2	2		4	1	1		20		10	5	12	57
{5,7}								1		2	1	3	7
{2,11}	2	36		1	6	6				12	2		65
{3,11}	2	6		9	3	3		6		12	6	3	50
{5,11}	2												2
{7,11}												3	3
{2,13}		60		1	10	10	7	2	1	12	2	7	112
{3,13}	4	2	4	16	1	1		32		16	8	12	96
{5,13}							3		1			3	7
{7,13}							3		1			12	16
{11,13}		2			1	1		1		2	1	3	11
{2,17}	12												12
{3,17}		4	2	4	2	2	3	5	1	10	5	3	41
{5,17}													0
{7,17}								1		2	1	3	7
{11,17}		2		1	1	1				4	2		11
{13,17}			2									3	5
{2,19}		78		3	13	13	7	3	1	18	3	7	146
{3,19}	2	4		4	2	2	3	20	1	10	5	12	65
{5,19}												3	3
{7,19}							3	4	1	2	1	12	23
{11,19}							3		1			3	7
{13,19}		2			1	1		4		2	1	12	23
{17,19}												3	3
{2,23}	4	54		3	9	9				18	3		100
{3,23}	8	6		9	3	3		6		12	6	3	56
{5,23}		2			1	1				2	1		7
{7,23}		2			1	1		1		2	1	3	11
{11,23}		2			1	1				2	1		7
{13,23}			2					1		2	1	3	9
{17,23}		2			1	1				2	1		7
{19,23}		2			1	1		1		2	1	3	11
{2,29}	2	102		3	17	17				18	3		162

continued on next page

TABLE A.2: Imprimitive sextics with $|S| = 2$ (*cont.)*

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{3,29}		8	2	9	4	4		6		12	6	3	54
{5,29}	2		4										6
{7,29}			2				3		1			3	9
{11,29}		2			1	1				2	1		7
{13,29}	8											3	11
{17,29}			2										2
{19,29}		2			1	1		1		2	1	3	11
{23,29}	2									2	1		5
{2,31}	2	18			3	3	35	1	5	6	1	7	81
{3,31}	2	4		9	2	2		24		12	6	12	73
{5,31}			2					1		2	1	3	9
{7,31}								4		2	1	12	19
{11,31}		4		1	2	2		2		4	2	3	20
{13,31}		2			1	1	3	4	1	2	1	12	27
{17,31}		4		1	2	2		2		4	2	3	20
{19,31}							3	4	1	2	1	12	23
{23,31}		2		1	1	1	3	2	1	4	2	3	20
{29,31}		2			1	1	3	1	1	2	1	3	15
{2,37}	4	60	2	1	10	10	7	2	1	12	2	7	118
{3,37}	28	2	2	16	1	1	3	32	1	16	8	12	122
{5,37}												3	3
{7,37}			2					4		2	1	12	21
{11,37}	2		2				3	1	1	2	1	3	15
{13,37}												12	12
{17,37}			2									3	5
{19,37}							6		2			12	20
{23,37}		2			1	1	3	1	1	2	1	3	15
{29,37}			4				3		1			3	11
{31,37}		8		1	4	4	6	8	2	4	2	12	51
{2,41}	8		2										10
{3,41}		10	2	4	5	5		5		10	5	3	49
{5,41}	4												4
{7,41}							3	1	1	2	1	3	11
{11,41}		6		1	3	3				4	2		19
{13,41}		2			1	1		1		2	1	3	11
{17,41}		8		1	4	4				4	2		23
{19,41}		6			3	3		1		2	1	3	19

continued on next page

Table A.2: Imprimitive sextics with $|S| = 2$ (*cont.)*

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{23,41}	2									2	1		5
{29,41}		2			1	1				2	1		7
{31,41}								1		2	1	3	7
{37,41}	4		2									3	9
{2,43}	2	36		1	6	6	35	2	5	12	2	7	114
{3,43}	2	6		4	3	3		20		10	5	12	65
{5,43}		2			1	1		1		2	1	3	11
{7,43}							3	4	1	2	1	12	23
{11,43}	2	6			3	3	3	1	1	2	1	3	25
{13,43}	2	2			1	1		4		2	1	12	25
{17,43}		6			3	3		1		2	1	3	19
{19,43}								4		2	1	12	19
{23,43}		2			1	1		1		2	1	3	11
{29,43}								1		2	1	3	7
{31,43}		2		1	1	1	3	8	1	4	2	12	35
{37,43}							3		1			12	16
{41,43}	2	2			1	1	3	1	1	2	1	3	17
{2,47}	6	36	2	1	6	6				12	2		71
{3,47}	8	10		9	5	5		6		12	6	3	64
{5,47}		6		1	3	3				4	2		19
{7,47}	2	2		1	1	1		2		4	2	3	18
{11,47}										2	1		3
{13,47}							3		1			3	7
{17,47}													0
{19,47}												3	3
{23,47}				1						4	2		7
{29,47}		4		1	2	2				4	2		15
{31,47}	2	6			3	3	3	1	1	2	1	3	25
{37,47}	2						3	1	1	2	1	3	13
{41,47}		2		1	1	1				4	2		11
{43,47}		6			3	3	3	1	1	2	1	3	23
{2,53}	2	126	4	3	21	21				18	3		198
{3,53}		2	2	4	1	1	3	5	1	10	5	3	37
{5,53}													0
{7,53}		6			3	3		1		2	1	3	19
{11,53}			2										2
{13,53}	2		2				3		1			3	11

continued on next page

Table A.2: Imprimitive sextics with $|S| = 2$ (*cont.)*

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{17,53}			2										2
{19,53}		2		1	1	1		2		4	2	3	16
{23,53}		10		3	5	5				6	3		32
{29,53}	2		2										4
{31,53}		2			1	1		4		8	4	3	23
{37,53}	8											3	11
{41,53}													0
{43,53}	2	6			3	3		1		2	1	3	21
{47,53}	4	2			1	1				2	1		11
{2,59}	2	144		6	24	24				24	4		228
{3,59}	8	4		9	2	2		6		12	6	3	52
{5,59}		2	2		1	1				2	1		9
{7,59}		4		4	2	2		5		10	5	3	35
{11,59}		2			1	1				2	1		7
{13,59}		2			1	1		1		2	1	3	11
{17,59}	2	6			3	3				2	1		17
{19,59}		4		1	2	2		2		4	2	3	20
{23,59}		8		1	4	4				4	2		23
{29,59}	4	2			1	1				2	1		11
{31,59}		6		1	3	3		2		4	2	3	24
{37,59}		8		1	4	4		2		4	2	3	28
{41,59}		2	2		1	1				2	1		9
{43,59}	8	6			3	3	3	1	1	2	1	3	31
{47,59}		2			1	1				2	1		7
{53,59}	2	4	2	1	2	2				4	2		19
{2,61}		60		1	10	10	7	2	1	12	2	7	112
{3,61}	28	4	2	16	2	2	3	32	1	16	8	12	126
{5,61}			4									3	7
{7,61}												12	12
{11,61}		2			1	1	3	1	1	2	1	3	15
{13,61}	4	6	4		3	3		4		2	1	12	39
{17,61}												3	3
{19,61}	2	2			1	1		4		2	1	12	25
{23,61}		4		1	2	2	3	2	1	4	2	3	24
{29,61}												3	3
{31,61}		2			1	1	3	4	1	2	1	12	27
{37,61}							3		1			12	16

continued on next page

Table A.2: Imprimitive sextics with $|S| = 2$ (*cont.*)

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{41,61}	2		2				3		1			3	11
{43,61}												12	12
{47,61}	2	8		1	4	4		2		4	2	3	30
{53,61}		6			3	3	3	1	1	2	1	3	23
{59,61}		4		1	2	2		2		4	2	3	20
{2,67}	8	36		1	6	6	7	2	1	12	2	7	88
{3,67}	2	12		4	6	6	3	20	1	10	5	12	81
{5,67}		4		1	2	2	3	2	1	4	2	3	24
{7,67}		6		1	3	3		8		4	2	12	39
{11,67}		2		1	1	1		2		4	2	3	16
{13,67}												12	12
{17,67}												3	3
{19,67}		2			1	1		4		2	1	12	23
{23,67}		2			1	1		1		2	1	3	11
{29,67}	2											3	5
{31,67}		6			3	3	3	4	1	2	1	12	35
{37,67}	2	8		1	4	4		8		4	2	12	45
{41,67}		4		1	2	2		2		4	2	3	20
{43,67}		6			3	3	6	4	2	2	1	12	39
{47,67}	2											3	5
{53,67}		6			3	3	3	1	1	2	1	3	23
{59,67}		2			1	1	3	1	1	2	1	3	15
{61,67}		2			1	1		4		2	1	12	23

Table A.3: Imprimitive sextics where S contains 3 primes.

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{2,3,5}	624	2002	44	375	143	143	15	31	1	434	31	15	3858
{2,3,7}	642	2100	28	345	150	150	120	120	8	420	30	60	4173
{2,5,7}	32	532	2	15	38	38	15	6	1	84	6	15	784
{3,5,7}	54	66	4	106	11	11	7	80	1	120	20	28	508
{2,3,11}	878	2394	8	493	171	171	15	35	1	490	35	15	4706
{2,5,11}	44	630	4	21	45	45				98	7		894
{3,5,11}	76	90	6	163	15	15		23		138	23	7	556
{2,7,11}	86	602	6	10	43	43	15	5	1	70	5	15	901

continued on next page

Table A.3: Imprimitive sextics with $|S| = 3$ (*cont.*)

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{3,7,11}	30	102		93	17	17	7	76	1	114	19	28	504
{5,7,11}	8	6		1	1	1		2		12	2	7	40
{2,3,13}	632	2100	46	345	150	150	120	120	8	420	30	60	4181
{2,5,13}	62	532	6	15	38	38	75	6	5	84	6	15	882
{3,5,13}	44	72	14	106	12	12	7	80	1	120	20	28	516
{2,7,13}	42	700	2	15	50	50	180	24	12	84	6	60	1225
{3,7,13}	76	78	6	87	13	13	21	247	3	114	19	91	768
{5,7,13}	4	12		1	2	2	14	8	2	12	2	28	87
{2,11,13}	48	1050	2	30	75	75	15	9	1	126	9	15	1455
{3,11,13}	46	120	24	147	20	20	7	88	1	132	22	28	655
{5,11,13}	6	30	2	3	5	5	7	3	1	18	3	7	90
{7,11,13}	2	30		3	5	5	14	12	2	18	3	28	122
{2,3,17}	852	2590	66	493	185	185	75	35	5	490	35	15	5026
{2,5,17}	70	644	8	15	46	46				84	6		919
{3,5,17}	44	108	14	147	18	18	7	22	1	132	22	7	540
{2,7,17}	108	546	6	10	39	39	15	5	1	70	5	15	859
{3,7,17}	54	90	4	106	15	15	7	80	1	120	20	28	540
{5,7,17}	2	12	2		2	2		4		24	4	7	59
{2,11,17}	74	714	4	30	51	51				126	9		1059
{3,11,17}	58	126	4	126	21	21	7	21	1	126	21	7	539
{5,11,17}	4	36	2	3	6	6				18	3		78
{7,11,17}	6	66		10	11	11		5		30	5	7	151
{2,13,17}	168	238	16	3	17	17	15	3	1	42	3	15	538
{3,13,17}	188	108	52	334	18	18	7	128	1	192	32	28	1106
{5,13,17}	14	6	6		1	1	7	1	1	6	1	7	51
{7,13,17}	2	30	4	3	5	5	14	12	2	18	3	28	126
{11,13,17}	4	24	4	6	4	4		4		24	4	7	85
{2,3,19}	894	2324	8	459	166	166	180	136	12	476	34	60	4915
{2,5,19}	48	672	2	22	48	48	15	8	1	112	8	15	999
{3,5,19}	64	108	4	147	18	18	14	88	2	132	22	28	645
{2,7,19}	46	518	2	15	37	37	180	28	12	98	7	60	1040
{3,7,19}	160	102		163	17	17	28	299	4	138	23	91	1042
{5,7,19}	4	24		3	4	4	14	12	2	18	3	28	116
{2,11,19}	85	1092		39	78	78	75	10	5	140	10	15	1627
{3,11,19}	30	96		75	16	16	14	72	2	108	18	28	475
{5,11,19}	44						7		1			7	59
{7,11,19}	10						35	4	5	6	1	28	89

continued on next page

TABLE A.3: Imprimitive sextics with $|S| = 3$ (*cont.)*

S	T_{13}	T_{11}	T_{10}	T_9	S_4^-	S_4^+	T_6	T_5	A_4	D_6	S_3	C_6	Total
{2,13,19}	54	798	2	21	57	57	120	28	8	98	7	60	1310
{3,13,19}	76	138	6	106	23	23	21	260	3	120	20	91	887
{5,13,19}	4	42	2	3	7	7	7	12	1	18	3	28	134
{7,13,19}	4	30		3	5	5	21	39	3	18	3	91	222
{11,13,19}	6	42		3	7	7	7	12	1	18	3	28	134
{2,17,19}	156	546	4	10	39	39	15	5	1	70	5	15	905
{3,17,19}	58	114	4	147	19	19	35	88	5	132	22	28	671
{5,17,19}	10	66	4	10	11	11		5		30	5	7	159
{7,17,19}	6	24	2	1	4	4	14	8	2	12	2	28	107
{11,17,19}	6	18	2	3	3	3	7	3	1	18	3	7	74
{13,17,19}	18	12	2	1	2	2	7	8	1	12	2	28	95

A.2. Imprimitive Octic Tables

We partition the imprimitive octics into 2 groups, those with a quartic subfield and those without a quartic subfield. For those octics having a quartic subfield, the fields were further partitioned into new and old fields. A field is said to be *old* if it's Galois closure is the compositum of smaller degree fields; otherwise, it is said to be *new*. Note that this definition differs slightly from that in [9]. The key point here is that old fields can be easily generated from tables of smaller degree fields by forming compositums and then computing the subfields of the compositums.

As a final note, if a column had no entries, then it was removed from the table. So if there is no column for a particular type of field, then that means that no fields of that type were found for all cases in that table.

Table A.4: Octics with a quartic subfield ($|S| = 1$).

S	T_1	T_2	T_4	T_6	T_7	T_8	T_{10}	T_{12}	T_{13}	T_{14}	T_{16}	T_{17}	T_{19}	T_{20}	T_{21}	T_{23}	T_{27}	T_{28}	T_{30}	T_{38}	T_{40}	Tot.
{2}	2	1	2	4	1	2	2				2	4	2	1	1		4	4	4			36
{3}																						0
{5}																						0
{7}																						0
{11}																						0
{13}																						0
{17}	1																					1
{19}																						0
{23}																						0
{29}																						0
{31}																						0
{37}																						0
{41}	1																					1
{43}																						0
{47}																						0
{53}																						0
{59}										1						2						3
{61}																						0
{67}																						0
{71}																						0
{73}	1																					1
{79}																						0
{83}																						0
{89}	1																					1
{97}	1																					1
{101}																						0
{103}																						0
{107}										1						2						3

continued on next page

TABLE A.4: Octics with a quartic subfield ($|S| = 1$). (*cont.*)

S	T_1	T_2	T_4	T_6	T_7	T_8	T_{10}	T_{12}	T_{13}	T_{14}	T_{16}	T_{17}	T_{19}	T_{20}	T_{21}	T_{23}	T_{27}	T_{28}	T_{30}	T_{38}	T_{40}	Tot.
{109}																						0
{113}	1																					1
{127}																						0
{131}																						0
{137}	1																					1
{139}										1						2						3
{149}																						0
{151}																						0
{157}																						0
{163}								2	1											4		7
{167}																						0
{173}																						0
{179}																						0
{181}																						0
{191}																						0
{193}	1																					1
{197}																						0
{199}																						0
{211}																						0
{223}																						0
{227}																						0
{229}										3											6	9

Table A.5: Old octics with a quartic subfield ($|S| = 2$).

S	T_2	T_3	T_4	T_9	T_{10}	T_{13}	T_{14}	T_{18}	T_{24}	Total
{2,3}	6	1	14	28	8	7	22	24	132	242
{2,5}	18	1	12	24	24		3	8	18	108
{3,5}	1						1		2	4
{2,7}	6	1	20	40	24	7		64		162
{3,7}			1				1		2	4
{5,7}	1									1
{2,11}	6	1	14	28	8		6	24	36	123
{3,11}			1				3		6	10
{5,11}	1		2		2					5
{7,11}			1							1
{2,13}	18	1	12	24	24	7	10	8	60	164
{3,13}	1		2		2		1		2	8
{5,13}	3					3				6
{7,13}	1					3				4
{11,13}	1						1		2	4
{2,17}	18	1	30	60	72			128		309
{3,17}	1					3	2		4	10
{5,17}	3									3
{7,17}	1									1
{11,17}	1						1		2	4
{13,17}	3		3		6					12
{2,19}	6	1	14	28	8	7	13	24	78	179
{3,19}			1			3	2		4	10
{5,19}	1		2		2					5
{7,19}			1			3				4
{11,19}			1			3				4
{13,19}	1						1		2	4
{17,19}	1		2		2					5
{2,23}	6	1	20	40	24		9	64	54	218
{3,23}			1				3		6	10
{5,23}	1						1		2	4
{7,23}			1				1		2	4
{11,23}			1				1		2	4
{13,23}	1		2		2					5
{17,23}	1						1		2	4
{19,23}			1				1		2	4
{2,29}	18	1	12	24	24		17	8	102	206

continued on next page

TABLE A.5: Old octics with a quartic subfield ($|S| = 2$). (*cont.)*

S	T_2	T_3	T_4	T_9	T_{10}	T_{13}	T_{14}	T_{18}	T_{24}	Total
{3,29}	1						4		8	13
{5,29}	3		3		6					12
{7,29}	1		2		2	3				8
{11,29}	1						1		2	4
{13,29}	3		3		6					12
{17,29}	3									3
{19,29}	1						1		2	4
{23,29}	1		2		2					5

TABLE A.6: New octics with a quartic subfield ($|S| = 2$).

S	T_1	T_5	T_6	T_7	T_8	T_{11}	T_{15}	T_{16}	T_{17}	T_{19}	T_{20}	T_{21}	T_{23}	T_{26}	T_{27}	T_{28}	T_{29}	T_{30}	T_{31}	T_{35}	T_{38}	T_{39}	T_{40}	T_{44}	Tot.
{2,3}	4	2	20	6	22	18	42	8	16	8	4	4	128	64	16	16	48	16	16	168	24	168	216	656	1690
{2,5}	8		20	20	10	18	42	24	72	24	12	12	24	24	48	48	24	48	8	72		24	24	96	702
{3,5}				1									4												5
{2,7}	4		60	6	16	12	68	24	48	24	12	12		176	48	48	120	48	40	480	24				1270
{3,7}					1								4												5
{5,7}				1																					1
{2,11}	4	2	20	6	22	18	42	8	16	8	4	4	40	64	16	16	48	16	16	168		24	32	240	834
{3,11}					1								8												9
{5,11}								2	4																6
{7,11}			2																						2
{2,13}	8		20	20	10	18	42	24	72	24	12	12	32	24	48	48	24	48	8	72	24	96	144	288	1118
{3,13}								2	4				4												10
{5,13}				2																					2
{7,13}				1																					1
{11,13}				1																					1
{2,17}	24	2	84	36	44	36	128	72	192	96	48	48		320	208	208	192	208	64	576					2586
{3,17}	2												8												10
{5,17}	4																								4
{7,17}	2																								2
{11,17}	2																								2
{13,17}	4	1		2				2	8	4	2	2			4	4									33
{2,19}	4	2	20	6	22	18	42	8	16	8	4	4	88	64	16	16	48	16	16	168	24	120	136	480	1346
{3,19}					1								8								4			8	21
{5,19}			2		1				2	2	1	1			2	2		4							17
{7,19}					1																4				5
{11,19}					1																4				5
{13,19}				1																					1
{17,19}	2		2	1	1				2																8
{2,23}	4		60	6	16	12	68	24	48	24	12	12	48	176	48	48	120	48	40	480		48	72	400	1814
{3,23}			2										8												10
{5,23}				1																					1
{7,23}			2																						2
{11,23}					1																				1
{13,23}			2		1				2	2	1	1			2	2		4							17
{17,23}	2																								2
{19,23}					1																				1
{2,29}	8		20	20	10	18	42	24	72	24	12	12	40	24	48	48	24	48	8	72		168	264	416	1422

continued on next page

TABLE A.6: New octics with a quartic subfield ($|S| = 2$). (*cont.*)

S	T_1	T_5	T_6	T_7	T_8	T_{11}	T_{15}	T_{16}	T_{17}	T_{19}	T_{20}	T_{21}	T_{23}	T_{26}	T_{27}	T_{28}	T_{29}	T_{30}	T_{31}	T_{35}	T_{38}	T_{39}	T_{40}	T_{44}	Tot.
{3,29}				1																			12		13
{5,29}		1							8	4	2	2			4	4									25
{7,29}								2	4																6
{11,29}				1									4											8	13
{13,29}		1						2	12	4	2	2			2	2		4							31
{17,29}	4																								4
{19,29}				1									4												5
{23,29}								2	4																6

TABLE A.7: Imprimitive octics with no quartic ($|S| = 1$).

S	T_{33}	T_{42}	Total
$\{2\}$			0
$\{3\}$			0
$\{5\}$			0
$\{7\}$			0
$\{11\}$			0
$\{13\}$			0
$\{17\}$			0
$\{19\}$			0
$\{23\}$			0
$\{29\}$			0
$\{31\}$			0
$\{37\}$			0
$\{41\}$			0
$\{43\}$			0
$\{47\}$			0
$\{53\}$			0
$\{59\}$			0
$\{61\}$			0
$\{67\}$			0
$\{71\}$			0
$\{73\}$			0
$\{79\}$			0
$\{83\}$			0
$\{89\}$			0
$\{97\}$			0
$\{101\}$			0
$\{103\}$			0
$\{107\}$			0
$\{109\}$			0
$\{113\}$			0
$\{127\}$			0
$\{131\}$			0
$\{137\}$			0
$\{139\}$		1	1
$\{149\}$			0
$\{151\}$			0
$\{157\}$			0

continued on next page

TABLE A.7: Imprimitive octics with no quartic ($|S| = 1$). (*cont.*)

S	T_{33}	T_{42}	Total
{163}	2		2
{167}			0
{173}			0
{179}			0
{181}			0
{191}			0

TABLE A.8: Imprimitive octics with no quartic ($|S| = 2$).

S	T_{33}	T_{34}	T_{41}	T_{42}	T_{45}	T_{46}	T_{47}	Total
{2,3}	6	11	90	12	110	28	542	799
{2,5}		1	12					13
{3,5}								0
{2,7}	6					14	22	42
{3,7}					1		1	2
{5,7}								0
{2,11}		2	40		3		22	67
{3,11}								0
{5,11}								0
{7,11}								0

We now give tables of specific octic fields. In the tables, L represents the octic field, d_L denotes the field discriminant, (r, s) is the signature, $G = \mathrm{Gal}(L^g/\mathbb{Q})$, h denotes the class number, and $\mathcal{C}_L$ denotes the class group. In the interest of saving space, and also because fields having larger class numbers are more interesting, Table A.11 only lists those fields having a class number greater than or equal to 100.

From Table A.9, one makes the interesting observation that every imprimitive octic ramified at only $p = 2$, has a trivial class group. On the other hand, Table A.11 gives examples of octics having highly non-trivial class groups; in fact, one octic even had a class number of 15076.

TABLE A.9: All imprimitive octics ramified at only $p = 2$.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
x^8+6x^4+1	2^{22}	(0,4)	T_4	1	C_1
x^8+1	2^{24}	(0,4)	T_2	1	C_1
$x^8-4x^6+8x^4-4x^2+1$	2^{24}	(0,4)	T_4	1	C_1
$x^8-4x^6+6x^4-4x^2+2$	2^{25}	(0,4)	T_{21}	1	C_1
$x^8+4x^6-2x^4+4x^2+1$	2^{26}	(0,4)	T_{10}	1	C_1
$x^8-4x^6-2x^4-4x^2+1$	2^{26}	(4,2)	T_{10}	1	C_1
$x^8+4x^4-4x^2+1$	2^{26}	(0,4)	T_9	1	C_1
$x^8-4x^6+10x^4-8x^2+2$	2^{27}	(0,4)	T_6	1	C_1
x^8-2x^4+2	2^{27}	(0,4)	T_{17}	1	C_1
x^8+2x^4+2	2^{27}	(0,4)	T_{17}	1	C_1
x^8-2x^4-1	-2^{28}	(2,3)	T_8	1	C_1
$x^8-6x^4-8x^2-1$	-2^{28}	(2,3)	T_6	1	C_1
$x^8-4x^6+10x^4+4x^2+1$	2^{28}	(0,4)	T_{19}	1	C_1
$x^8-4x^6-2x^4+12x^2+1$	2^{28}	(4,2)	T_{20}	1	C_1
$x^8+4x^6+4x^4-2$	-2^{29}	(2,3)	T_{30}	1	C_1
$x^8-4x^6+4x^4-2$	-2^{29}	(2,3)	T_{30}	1	C_1
$x^8-4x^6+8x^4-8x^2+2$	2^{29}	(4,2)	T_{28}	1	C_1
$x^8+4x^6+8x^4+8x^2+2$	2^{29}	(0,4)	T_{28}	1	C_1
$x^8-4x^6+2x^4+4x^2-1$	-2^{30}	(6,1)	T_{27}	1	C_1
$x^8+4x^6+2x^4-4x^2-1$	-2^{30}	(2,3)	T_{27}	1	C_1
$x^8-4x^6+6x^4-4x^2-1$	-2^{30}	(2,3)	T_{30}	1	C_1
$x^8+4x^6+6x^4+4x^2-1$	-2^{30}	(2,3)	T_{30}	1	C_1
x^8-2	-2^{31}	(2,3)	T_8	1	C_1
x^8-8x^4-2	-2^{31}	(2,3)	T_6	1	C_1
$x^8-8x^4-8x^2-2$	-2^{31}	(2,3)	T_{27}	1	C_1
$x^8-8x^4+8x^2-2$	-2^{31}	(6,1)	T_{27}	1	C_1
$x^8+8x^6+20x^4+16x^2+2$	2^{31}	(0,4)	T_1	1	C_1
$x^8-8x^6+20x^4-16x^2+2$	2^{31}	(8,0)	T_1	1	C_1
x^8+2	2^{31}	(0,4)	T_6	1	C_1
$x^8-8x^6-12x^4+2$	2^{31}	(4,2)	T_7	1	C_1
x^8-4x^4+2	2^{31}	(4,2)	T_{16}	1	C_1
x^8+4x^4+2	2^{31}	(0,4)	T_{16}	1	C_1
$x^8-8x^6+24x^4-32x^2+18$	2^{31}	(0,4)	T_{17}	1	C_1
$x^8+8x^6+24x^4+32x^2+18$	2^{31}	(0,4)	T_{17}	1	C_1
$x^8-4x^4+8x^2+2$	2^{31}	(0,4)	T_{28}	1	C_1
$x^8-4x^4-8x^2+2$	2^{31}	(4,2)	T_{28}	1	C_1

Table A.10: All octics from Tables A.4 and A.7 for $p > 2$.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8 - x^7 - 7x^6 + 6x^5 + 15x^4 - 10x^3 - 10x^2 + 4x + 1$	17^7	(8,0)	T_1	1	C_1
$x^8 - x^7 + 3x^6 - 11x^5 + 44x^4 + 53x^3 + 153x^2 + 160x + 59$	41^7	(0,4)	T_1	1	C_1
$x^8 - x^7 + x^6 + 5x^5 - x^4 + 10x^3 + 4x^2 - 8x + 16$	59^6	(0,4)	T_{14}	3	C_3
$x^8 - 3x^7 + 15x^6 - 26x^5 - 21x^4 - 35x^3 + 25x^2 + 50x + 29$	-59^7	(2,3)	T_{23}	1	C_1
$x^8 - 4x^7 + 7x^6 - 7x^5 - 3x^4 + 13x^3 - 136x^2 + 129x - 115$	-59^7	(2,3)	T_{23}	1	C_1
$x^8 - x^7 + 5x^6 + 17x^5 - 46x^4 + 136x^3 + 320x^2 - 512x + 4096$	73^7	(0,4)	T_1	89	C_{89}
$x^8 - x^7 + 6x^6 - 46x^5 - 143x^4 + 575x^3 + 1160x^2 - 16x + 512$	89^7	(0,4)	T_1	113	C_{113}
$x^8 - x^7 - 42x^6 + 59x^5 + 497x^4 - 719x^3 - 1792x^2 + 2295x + 193$	97^7	(8,0)	T_1	1	C_1
$x^8 - 8x^6 + 24x^4 + 75x^2 + 16$	107^6	(0,4)	T_{14}	3	C_3
$x^8 - 4x^7 + 7x^6 - 7x^5 - 9x^4 + 25x^3 + 74x^2 - 87x - 28$	-107^7	(2,3)	T_{23}	1	C_1
$x^8 - 3x^7 + 24x^6 - 18x^5 + 82x^4 + 596x^3 - 299x^2 + 4377x - 792$	-107^7	(2,3)	T_{23}	1	C_1
$x^8 - x^7 - 49x^6 - 16x^5 + 511x^4 + 367x^3 - 1499x^2 - 798x + 1372$	113^7	(8,0)	T_1	1	C_1
$x^8 - x^7 + 9x^6 - 105x^5 + 954x^4 - 3767x^3 + 9149x^2 - 12828x + 7607$	137^7	(0,4)	T_1	17	C_{17}
$x^8 - x^7 - x^6 + 14x^5 + 80x^4 + 56x^3 - 16x^2 - 64x + 256$	139^6	(0,4)	T_{14}	3	C_3
$x^8 - 2x^7 + 8x^6 - 24x^5 + 72x^4 - 137x^3 + 135x^2 - 68x + 16$	139^6	(0,4)	T_{42}	6	C_6
$x^8 - 4x^7 + 7x^6 - 7x^5 - 13x^4 + 33x^3 - 182x^2 + 165x - 436$	-139^7	(2,3)	T_{23}	1	C_1
$x^8 - 4x^7 + 7x^6 + 132x^5 - 708x^4 + 2952x^3 - 5881x^2 + 10312x - 3355$	-139^7	(2,3)	T_{23}	1	C_1
$x^8 - x^7 + x^6 - 4x^5 + 5x^4 - 8x^3 + 4x^2 - 8x + 16$	163^4	(0,4)	T_{12}	1	C_1
$x^8 - x^7 - 11x^6 + 39x^5 - 49x^4 - 8x^3 + 70x^2 - 47x + 8$	-163^5	(6,1)	T_{38}	1	C_1
$x^8 - x^7 - 12x^6 + 13x^5 + 29x^4 - 28x^3 - 25x^2 + 17x + 9$	-163^5	(6,1)	T_{38}	1	C_1
$x^8 - 3x^7 + 2x^6 + x^5 - 48x^4 + 96x^3 + 32x^2 + 80x - 224$	-163^5	(2,3)	T_{38}	3	C_3
$x^8 - 3x^7 + 6x^6 - 9x^5 + 25x^4 - 31x^3 - x^2 + 39x - 19$	-163^5	(2,3)	T_{38}	1	C_1
$x^8 - x^7 - 44x^6 + 43x^5 + 442x^4 - 32x^3 - 1311x^2 - 1156x - 241$	163^6	(8,0)	T_{12}	1	C_1
$x^8 - 3x^7 + 41x^6 - 35x^5 + 303x^4 + 241x^3 + 1094x^2 + 1865x + 1681$	163^6	(0,4)	T_{13}	12	C_6C_2
$x^8 - x^7 - 84x^6 + 21x^5 + 1981x^4 - 63x^3 - 14652x^2 + 799x + 30961$	193^7	(8,0)	T_1	1	C_1

continued on next page

TABLE A.10: All octics from Tables A.4 and A.7 for $p > 2$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8 - x^7 + 4x^5 - 2x^4 + 3x^2 - x + 1$	229^3	(0,4)	T_{40}	1	C_1
$x^8 + 4x^6 - 14x^5 + 35x^4 - 28x^3 + 111x^2 - 217x + 183$	229^4	(0,4)	T_{14}	3	C_3
$x^8 - 57x^5 + 86x^4 - 229x^3 - 161x^2 - 848x + 48565$	229^5	(0,4)	T_{40}	2	C_2
$x^8 + 16x^6 + 96x^4 + 27x^2 + 256$	229^6	(0,4)	T_{14}	12	C_{12}
$x^8 + 12x^6 + 54x^4 - 121x^2 + 81$	229^6	(0,4)	T_{14}	12	C_{12}
$x^8 - 4x^7 + 7x^6 - 7x^5 + 262x^4 - 517x^3 + 759x^2 - 501x + 3223$	229^7	(0,4)	T_{40}	8	C_8
$x^8 - 229x^2 + 916$	229^7	(0,4)	T_{40}	8	C_8
$x^8 - 4x^7 + 7x^6 - 7x^5 + 720x^4 - 1433x^3 + 1446x^2 - 730x + 124593$	229^7	(0,4)	T_{40}	8	C_8
$x^8 - 4x^7 + 7x^6 - 7x^5 + 33x^4 - 59x^3 + 72x^2 - 43x + 17$	229^7	(0,4)	T_{40}	8	C_8

TABLE A.11: All octics from Tables A.5, A.6, and A.8 having class number $h \geq 100$.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8 - x^7 + 78x^6 - 79x^5 + 1375x^4 - 2645x^3 + 9170x^2 - 18951x + 26351$	$17^7 19^4$	(0,4)	T_1	100	$C_{10}C_{10}$
$x^8 + 56x^6 + 980x^4 + 5488x^2 + 16129$	$2^{24}29^4$	(0,4)	T_2	102	C_{102}
$x^8 + 68x^6 + 816x^4 + 3468x^2 + 4913$	$2^{24}17^5$	(0,4)	T_{17}	104	$C_{26}C_2C_2$
$x^8 + 68x^6 + 1394x^4 + 9248x^2 + 18496$	$2^{22}17^6$	(0,4)	T_2	104	$C_{26}C_2C_2$
$x^8 + 28x^6 + 158x^4 - 328x^2 + 4356$	$2^{22}17^6$	(0,4)	T_{10}	104	$C_{52}C_2$
$x^8 + 56x^6 + 672x^4 + 2352x^2 + 2450$	$2^{31}7^6$	(0,4)	T_{17}	104	$C_{26}C_2C_2$
$x^8 - 2x^7 + 12x^6 - 12x^5 + 172x^4 - 244x^3 + 1703x^2 - 1390x + 5252$	$17^6 23^4$	(0,4)	T_2	105	C_{105}
$x^8 + 4x^6 + 10x^4 - 4x^2 + 529$	$2^{28}29^4$	(0,4)	T_{39}	112	C_{112}
$x^8 + 16x^6 + 208x^4 + 1024x^2 + 1472$	$2^{30}23^5$	(0,4)	T_{44}	120	$C_{60}C_2$
$x^8 - 4x^7 - 8x^6 + 4x^5 + 432x^4 - 524x^3 - 3328x^2 - 1996x + 31361$	$2^{22}17^6$	(0,4)	T_4	128	$C_8C_4C_2C_2$
$x^8 - 4x^7 + 60x^6 - 132x^5 + 840x^4 - 660x^3 + 1772x^2 - 500x + 81$	$2^{22}17^6$	(0,4)	T_4	128	$C_4C_4C_4C_2$
$x^8 - 8x^6 + 92x^4 + 784x^2 + 1444$	$2^{24}17^6$	(0,4)	T_9	128	$C_8C_8C_2$
$x^8 + 4x^6 + 40x^4 + 4x^2 + 1$	$2^{24}17^6$	(0,4)	T_{18}	128	$C_8C_8C_2$
$x^8 - 4x^6 + 40x^4 - 4x^2 + 1$	$2^{24}17^6$	(0,4)	T_{18}	128	$C_8C_8C_2$
$x^8 + 4x^6 - 62x^4 + 412x^2 + 1089$	$2^{24}17^6$	(0,4)	T_4	128	$C_8C_4C_2C_2$
$x^8 + 8x^6 - 44x^4 + 848x^2 + 900$	$2^{24}17^6$	(0,4)	T_9	128	$C_8C_4C_2C_2$
$x^8 + 12x^6 - 82x^4 + 108x^2 + 81$	$2^{26}17^6$	(0,4)	T_{18}	128	$C_8C_4C_2C_2$
$x^8 + 12x^6 + 122x^4 + 516x^2 + 625$	$2^{26}17^6$	(0,4)	T_{18}	128	$C_{16}C_2C_2C_2$
$x^8 + 510x^4 + 544x^2 + 425$	$2^{22}17^7$	(0,4)	T_{26}	128	$C_{16}C_4C_2$
$x^8 - 68x^4 + 2176x^2 - 4352x + 3332$	$2^{24}17^7$	(0,4)	T_{35}	128	$C_{16}C_2C_2C_2$
$x^8 + 68x^4 + 4352x^2 + 35972$	$2^{24}17^7$	(0,4)	T_{35}	128	$C_{16}C_4C_2$
$x^8 + 136x^2 + 425$	$2^{24}17^7$	(0,4)	T_{26}	128	$C_{16}C_4C_2$
$x^8 + 136x^4 - 544x^3 + 816x^2 - 544x + 136$	$2^{26}17^7$	(0,4)	T_{35}	128	$C_8C_4C_4$
$x^8 + 68x^4 - 1088x^2 + 3332$	$2^{26}17^7$	(0,4)	T_{35}	128	$C_{16}C_2C_2C_2$
$x^8 + 68x^4 + 68x^2 + 17$	$2^{26}17^7$	(0,4)	T_{35}	128	$C_{16}C_4C_2$

continued on next page

TABLE A.11: All octics from Tables A.5, A.6, and A.8 having class number $h \geq 100$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8 + 272x^4 - 544x^2 + 272$	$2^{26}17^7$	(0,4)	T_{35}	128	$C_{16}C_4C_2$
$x^8 + 16x^6 + 96x^4 + 256x^2 + 800$	$2^{31}17^6$	(0,4)	T_{35}	128	$C_8C_4C_4$
$x^8 - 16x^6 + 96x^4 - 256x^2 + 800$	$2^{31}17^6$	(0,4)	T_{35}	128	$C_8C_4C_4$
$x^8 + 306x^4 - 8976x^2 + 171394$	$2^{27}17^7$	(0,4)	T_{17}	128	$C_{16}C_2C_2C_2$
$x^8 - 68x^6 + 1190x^4 - 4896x^2 + 134946$	$2^{27}17^7$	(0,4)	T_{15}	128	$C_{16}C_4C_2$
$x^8 + 68x^6 + 1190x^4 + 4896x^2 + 134946$	$2^{27}17^7$	(0,4)	T_{15}	128	$C_8C_4C_2C_2$
$x^8 + 1020x^4 - 8160x^2 + 16456$	$2^{27}17^7$	(0,4)	T_{17}	128	$C_{16}C_2C_2C_2$
$x^8 + 204x^4 - 2448x^2 + 6664$	$2^{27}17^7$	(0,4)	T_6	128	$C_{16}C_2C_2C_2$
$x^8 + 612x^4 + 8160x^2 + 71944$	$2^{27}17^7$	(0,4)	T_{17}	128	$C_8C_4C_4$
$x^8 - 68x^6 + 986x^4 + 5508x^2 + 67473$	$2^{28}17^7$	(0,4)	T_{35}	128	$C_{16}C_8$
$x^8 - 68x^6 + 918x^4 + 8092x^2 + 14297$	$2^{28}17^7$	(0,4)	T_{35}	128	$C_{16}C_8$
$x^8 + 68x^6 + 986x^4 - 5508x^2 + 67473$	$2^{28}17^7$	(0,4)	T_{35}	128	$C_{16}C_8$
$x^8 + 68x^6 + 918x^4 - 8092x^2 + 14297$	$2^{28}17^7$	(0,4)	T_{35}	128	$C_{16}C_8$
$x^8 + 2040x^4 - 8160x^2 + 12274$	$2^{31}17^7$	(0,4)	T_{26}	128	$C_8C_8C_2$
$x^8 - 544$	$-2^{31}17^7$	(2,3)	T_{15}	128	$C_8C_8C_2$
$x^8 - 34$	$-2^{31}17^7$	(2,3)	T_{15}	128	$C_8C_4C_2C_2$
$x^8 + 272x^4 + 2448x^2 + 21250$	$2^{31}17^7$	(0,4)	T_{26}	128	$C_8C_8C_2$
$x^8 + 816x^4 - 136$	$-2^{31}17^7$	(2,3)	T_6	128	$C_8C_4C_4$
$x^8 + 272x^4 + 21250$	$2^{31}17^7$	(0,4)	T_6	128	$C_{16}C_2C_2C_2$
$x^8 - 544x^4 - 6800x^2 - 21250$	$-2^{31}17^7$	(2,3)	T_{26}	128	$C_8C_4C_4$
$x^8 + 272x^4 - 2448x^2 + 21250$	$2^{31}17^7$	(0,4)	T_{26}	128	$C_8C_8C_2$
$x^8 + 2040x^4 + 8160x^2 + 12274$	$2^{31}17^7$	(0,4)	T_{26}	128	$C_8C_8C_2$
$x^8 - 544x^4 + 6800x^2 - 21250$	$-2^{31}17^7$	(2,3)	T_{26}	128	$C_8C_4C_4$
$x^8 - 680x^4 + 9520x^2 - 37026$	$-2^{31}17^7$	(2,3)	T_{26}	128	$C_8C_4C_4$
$x^8 - 1288x^4 + 190440x^2 + 24334$	$2^{31}23^5$	(0,4)	T_{35}	128	$C_{32}C_4$

continued on next page

TABLE A.11: All octics from Tables A.5, A.6, and A.8 having class number $h \geq 100$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8 - x^7 + 90x^6 - 360x^5 + 2693x^4 - 8436x^3 - 36016x^2 + 125865x + 600903$	$17^6 29^6$	(0,4)	T_2	130	C_{130}
$x^8 + 32x^6 + 276x^4 + 920x^2 + 1058$	$2^{31} 23^4$	(0,4)	T_{28}	132	$C_{66}C_2$
$x^8 + 32x^6 + 256x^4 + 552x^2 + 46$	$2^{31} 23^5$	(0,4)	T_{27}	132	$C_{66}C_2$
$x^8 + 34x^6 + 374x^4 + 1360x^2 + 544$	$2^{19} 17^7$	(0,4)	T_6	136	$C_{68}C_2$
$x^8 + 68x^6 + 1394x^4 + 7888x^2 + 272$	$2^{22} 17^7$	(0,4)	T_1	136	$C_{68}C_2$
$x^8 + 32x^6 + 350x^4 - 136x^3 + 1232x^2 - 1224x + 1631$	$2^{26} 17^6$	(0,4)	T_{20}	144	$C_{36}C_2C_2$
$x^8 + 68x^6 + 646x^4 + 1156x^2 + 289$	$2^{26} 17^6$	(0,4)	T_{19}	144	$C_{36}C_2C_2$
$x^8 + 40x^6 + 552x^4 + 2944x^2 + 4232$	$2^{31} 23^4$	(0,4)	T_{28}	144	$C_{72}C_2$
$x^8 + 40x^6 + 400x^4 + 736x^2 + 184$	$2^{31} 23^5$	(0,4)	T_{27}	144	$C_{72}C_2$
$x^8 + 64x^6 + 696x^4 + 1856x^2 + 928$	$2^{27} 29^5$	(0,4)	T_{44}	156	C_{156}
$x^8 + 68x^6 + 1564x^4 + 13872x^2 + 39304$	$2^{25} 17^5$	(0,4)	T_{30}	160	$C_{40}C_2C_2$
$x^8 + 68x^6 + 1326x^4 + 5780x^2 + 4913$	$2^{28} 17^5$	(0,4)	T_{30}	160	$C_{40}C_2C_2$
$x^8 + 8x^6 + 760x^4 + 32x^2 + 16$	$2^{26} 23^6$	(0,4)	T_{18}	160	$C_{40}C_4$
$x^8 - 8x^6 + 760x^4 - 32x^2 + 16$	$2^{26} 23^6$	(0,4)	T_{18}	160	$C_{40}C_4$
$x^8 + 64x^6 + 1288x^4 + 8128x^2 + 928$	$2^{27} 29^5$	(0,4)	T_{44}	160	C_{160}
$x^8 + 104x^6 + 3380x^4 + 35152x^2 + 57122$	$2^{31} 13^4$	(0,4)	T_1	162	$C_{18}C_9$
$x^8 + 152x^6 + 380x^4 + 304x^2 + 76$	$2^{28} 19^7$	(0,4)	T_8	162	$C_{18}C_9$
$x^8 - 3x^7 + 71x^6 - 568x^5 + 4464x^4 - 18600x^3 + 68723x^2 - 129825x + 209173$	$13^5 29^7$	(0,4)	T_{17}	164	$C_{82}C_2$
$x^8 - x^7 + 61x^6 - 708x^5 + 2548x^4 + 15460x^3 - 34537x^2 - 198471x + 1275443$	$17^7 29^6$	(0,4)	T_1	164	C_{164}
$x^8 + 40x^6 + 500x^4 + 2000x^2 + 2450$	$2^{31} 5^6$	(0,4)	T_1	164	C_{164}
$x^8 + 88x^6 + 2684x^4 + 32912x^2 + 128018$	$2^{31} 11^6$	(0,4)	T_7	170	C_{170}
$x^8 + 116x^6 + 2030x^4 + 6728x^2 + 3364$	$2^{22} 29^6$	(0,4)	T_2	170	C_{170}
$x^8 + 272x^4 - 2754$	$-2^{31} 17^7$	(2,3)	T_8	192	$C_{48}C_4$
$x^8 + 8x^6 - 32x^5 + 110x^4 - 1520x^3 + 5620x^2 - 7304x + 3630$	$2^{24} 29^6$	(0,4)	T_{24}	192	$C_{96}C_2$
$x^8 + 68x^6 + 1530x^4 + 11424x^2 + 1088$	$2^{22} 17^7$	(0,4)	T_7	200	$C_{20}C_{10}$

continued on next page

TABLE A.11: All octics from Tables A.5, A.6, and A.8 having class number $h \geq 100$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8+92x^6+2898x^4+38088x^2+178802$	$2^{27}23^6$	(0,4)	T_8	204	$C_{102}C_2$
$x^8+348x^4-33640x^2+613089$	$2^{24}29^6$	(0,4)	T_2	204	C_{204}
$x^8-72x^6+1654x^4-1624x^3+568x^2-17864x+29199$	$2^{26}29^6$	(0,4)	T_{10}	204	C_{204}
$x^8+76x^6+2030x^4+19276x^2+7921$	$2^{26}17^6$	(0,4)	T_{10}	208	$C_{52}C_2C_2$
$x^8-20x^6+422x^4-3220x^2+12321$	$2^{26}17^6$	(0,4)	T_{10}	208	$C_{52}C_2C_2$
$x^8-1020x^4-2720x^2+333234$	$2^{31}17^7$	(0,4)	T_{16}	208	$C_{104}C_2$
$x^8+68x^4-7344x^2+68850$	$2^{31}17^7$	(0,4)	T_{16}	208	$C_{104}C_2$
$x^8-1020x^4+2720x^2+333234$	$2^{31}17^7$	(0,4)	T_{16}	208	$C_{104}C_2$
$x^8+68x^4+7344x^2+68850$	$2^{31}17^7$	(0,4)	T_{16}	208	$C_{104}C_2$
$x^8+88x^6+2420x^4+21296x^2+29282$	$2^{31}11^4$	(0,4)	T_1	226	C_{226}
$x^8+92x^6+3036x^4+42320x^2+207368$	$2^{25}23^6$	(0,4)	T_{21}	248	$C_{62}C_2C_2$
$x^8+92x^6+2116x^4+4232x^2+2116$	$2^{26}23^6$	(0,4)	T_{19}	248	$C_{124}C_2$
$x^8+92x^6+2254x^4+6348x^2+529$	$2^{28}23^6$	(0,4)	T_{20}	248	$C_{124}C_2$
$x^8+92x^6+1978x^4+2116x^2+529$	$2^{28}23^6$	(0,4)	T_{19}	248	$C_{62}C_2C_2$
$x^8+1326x^4+8976x^2+32674$	$2^{27}17^7$	(0,4)	T_{17}	256	$C_{16}C_4C_4$
$x^8+68x^6+1088x^4-1088x^2+850$	$2^{29}17^7$	(0,4)	T_{28}	256	$C_{16}C_8C_2$
$x^8-272x^4+21250$	$2^{31}17^7$	(0,4)	T_6	256	$C_{16}C_4C_4$
$x^8-4x^7+24x^6-24x^5+474x^4-992x^3+1540x^2-6000x+6750$	$2^{22}17^7$	(0,4)	T_6	272	$C_{136}C_2$
$x^8+136x^6+5508x^4+66096x^2+24786$	$2^{31}17^7$	(0,4)	T_1	272	$C_{136}C_2$
$x^8+152x^6+7220x^4+109744x^2+260642$	$2^{31}19^4$	(0,4)	T_1	274	C_{274}
$x^8+348x^4+8584x^2+4698$	$2^{31}29^7$	(0,4)	T_{28}	276	C_{276}
$x^8+2720x^4-27744x^2+1223048$	$2^{31}17^6$	(0,4)	T_{17}	288	$C_{24}C_6C_2$
$x^8+116x^6+1450x^4+4408x^2+2900$	$2^{22}29^7$	(0,4)	T_7	290	C_{290}
$x^8+104x^6+3380x^4+35152x^2+97682$	$2^{31}13^6$	(0,4)	T_1	292	C_{292}
$x^8-x^7+10x^6+6x^5+49x^4-129x^3+500x^2+2044x+1616$	$5^6 17^7$	(0,4)	T_1	292	C_{292}

continued on next page

TABLE A.11: All octics from Tables A.5, A.6, and A.8 having class number $h \geq 100$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8+76x^6+1710x^4+12312x^2+27702$	$2^{27}19^7$	(0,4)	T_8	306	C_{306}
$x^8+136x^6+6460x^4+124848x^2+795906$	$2^{31}17^5$	(0,4)	T_{17}	320	$C_{40}C_4C_2$
$x^8+68x^6+578x^4+1360x^2+272$	$2^{22}17^7$	(0,4)	T_1	328	$C_{164}C_2$
$x^8+152x^6+7676x^4+144400x^2+693842$	$2^{31}19^6$	(0,4)	T_7	338	C_{338}
$x^8+104x^6+3380x^4+35152x^2+4394$	$2^{31}13^7$	(0,4)	T_7	388	C_{388}
$x^8+136x^6+5780x^4+78608x^2+167042$	$2^{31}17^4$	(0,4)	T_1	400	$C_{10}C_{10}C_2C_2$
$x^8+136x^6+6188x^4+106352x^2+481474$	$2^{31}17^5$	(0,4)	T_{17}	400	$C_{100}C_2C_2$
$x^8-4x^7-60x^6-36x^5+1264x^4+5884x^3+12116x^2+12460x+5225$	$2^{22}23^6$	(0,4)	T_4	400	$C_{40}C_{10}$
$x^8+40x^6+260x^4+464x^2+225$	$2^{24}17^6$	(0,4)	T_{10}	416	$C_{104}C_2C_2$
$x^8-272x^4+83521$	$2^{24}17^6$	(0,4)	T_2	416	$C_{52}C_4C_2$
$x^8+816x^4-4624x^2+23409$	$2^{24}17^6$	(0,4)	T_2	416	$C_{52}C_4C_2$
$x^8+60x^6+1758x^4+19484x^2+50625$	$2^{26}17^6$	(0,4)	T_{10}	416	$C_{104}C_2C_2$
$x^8-44x^6+624x^4-680x^3+1544x^2-4080x+4050$	$2^{26}17^6$	(0,4)	T_{10}	416	$C_{104}C_2C_2$
$x^8+52x^4+104x^2+26$	$2^{31}13^7$	(0,4)	T_{44}	432	$C_{108}C_2C_2$
x^8+68x^4+5508	$2^{24}17^7$	(0,4)	T_6	448	$C_{112}C_4$
$x^8+92x^6+2668x^4+25392x^2+24334$	$2^{29}23^5$	(0,4)	T_{30}	464	$C_{232}C_2$
$x^8+92x^6+2622x^4+23276x^2+12167$	$2^{30}23^5$	(0,4)	T_{30}	464	$C_{116}C_2C_2$
$x^8+104x^6+3380x^4+35152x^2+109850$	$2^{31}13^7$	(0,4)	T_7	484	$C_{44}C_{11}$
$x^8+4x^6+74x^4-404x^2+1225$	$2^{24}17^6$	(0,4)	T_4	512	$C_8C_8C_4C_2$
x^8+136	$2^{31}17^7$	(0,4)	T_{15}	512	$C_{16}C_8C_2C_2$
x^8+2176	$2^{31}17^7$	(0,4)	T_{15}	512	$C_{16}C_{16}C_2$
$x^8+68x^6+340x^4+476x^2+153$	$2^{24}17^7$	(0,4)	T_8	528	$C_{264}C_2$
$x^8+184x^6+4048x^4+25392x^2+26450$	$2^{31}23^6$	(0,4)	T_{17}	584	$C_{146}C_2C_2$
$x^8+136x^6+5780x^4+78608x^2+305762$	$2^{31}17^6$	(0,4)	T_1	656	$C_{164}C_2C_2$
$x^8+136x^6+3332x^4+26928x^2+68850$	$2^{31}17^7$	(0,4)	T_1	656	$C_{328}C_2$

continued on next page

TABLE A.11: All octics from Tables A.5, A.6, and A.8 having class number $h \geq 100$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^8+136x^6+6596x^4+134096x^2+971618$	$2^{31}17^6$	(0,4)	T_7	720	$C_{60}C_6C_2$
$x^8+116x^6+3422x^4+5104x^2+1682$	$2^{27}29^6$	(0,4)	T_{23}	768	$C_{384}C_2$
$x^8+116x^6+4930x^4+90712x^2+607202$	$2^{27}29^6$	(0,4)	T_{23}	768	$C_{384}C_2$
$x^8-x^7+89x^6+98x^5+2059x^4+1787x^3+11399x^2-1884x+34308$	$13^7 29^5$	(0,4)	T_{17}	808	$C_{202}C_2C_2$
$x^8+184x^6+2208x^4+8464x^2+9522$	$2^{31}23^6$	(0,4)	T_{17}	808	$C_{202}C_2C_2$
$x^8+104x^6+3380x^4+35152x^2+16562$	$2^{31}13^6$	(0,4)	T_1	964	C_{964}
$x^8+184x^6+10580x^4+194672x^2+559682$	$2^{31}23^4$	(0,4)	T_1	1028	$C_{514}C_2$
x^8-272x^4-2754	$-2^{31}17^7$	(2,3)	T_8	1088	$C_{272}C_4$
$x^8+136x^6+5780x^4+78608x^2+28322$	$2^{31}17^6$	(0,4)	T_1	1296	$C_{36}C_{18}C_2$
$x^8+232x^6+16820x^4+390224x^2+2390122$	$2^{31}29^7$	(0,4)	T_7	1300	C_{1300}
$x^8+232x^6+16820x^4+390224x^2+1414562$	$2^{31}29^4$	(0,4)	T_1	1394	C_{1394}
$x^8+136x^6+5780x^4+78608x^2+850$	$2^{31}17^7$	(0,4)	T_7	1424	$C_{712}C_2$
$x^8+232x^6+16820x^4+390224x^2+2827442$	$2^{31}29^6$	(0,4)	T_1	1700	$C_{340}C_5$
$x^8+136x^6+5780x^4+78608x^2+333234$	$2^{31}17^7$	(0,4)	T_7	1744	$C_{872}C_2$
$x^8+232x^6+16820x^4+390224x^2+1682$	$2^{31}29^6$	(0,4)	T_1	2372	C_{2372}
$x^8-x^7+27x^6+125x^5-308x^4-2628x^3+2336x^2+35840x+65536$	$13^6 17^7$	(0,4)	T_1	2448	$C_{204}C_6C_2$
$x^8+136x^6+4964x^4+56304x^2+68850$	$2^{31}17^7$	(0,4)	T_1	2448	$C_{408}C_6$
$x^8+232x^6+16820x^4+390224x^2+2485242$	$2^{31}29^7$	(0,4)	T_7	4100	$C_{820}C_5$
$x^8+136x^6+2788x^4+17136x^2+24786$	$2^{31}17^7$	(0,4)	T_1	11152	$C_{5576}C_2$
$x^8-x^7+61x^6-215x^5+3534x^4+7572x^3-47848x^2+576032x+2332928$	$17^7 29^6$	(0,4)	T_1	15076	C_{15076}

A.3. Imprimitive Nonic Tables

We now provide complete tables for imprimitive fields of degree 9. For cases having more than 2 primes, we partition the data into new and old fields.

Tables A.12, A.13, and A.14 give numbers of each type of field for various sets S. As in previous cases, if a column does not exist for a specific type of field then that means that no fields of that type were found for all cases in that table.

Tables A.15 and A.16 give specific field data, ordered by increasing class number. In the interest of saving space, Table A.16 only lists those fields having a class number greater than or equal to 8.

Table A.12: Imprimitive nonics where S contains 1 prime.

S	T_1	T_3	T_4	T_{10}	T_{11}	T_{13}	T_{20}	T_{22}	T_{28}	Total
{2}										0
{3}	1	1	1	2	1	1	3	3		13
{5}										0
{7}										0
{11}										0
{13}										0
{17}										0
{19}	1									1
{23}										0
{29}										0
{31}			1	1						2
{37}	1									1
{41}										0
{43}										0
{47}										0
{53}										0
{59}										0
{61}										0
{67}										0
{71}										0
{73}	1									1
{79}										0
{83}										0
{89}										0
{97}										0
{101}										0
{103}										0

continued on next page

Table A.12: Imprimitive nonics with $|S| = 1$ (*cont.)*

S	T_1	T_3	T_4	T_{10}	T_{11}	T_{13}	T_{20}	T_{22}	T_{28}	Total
{107}										0
{109}	1									1
{113}										0
{127}	1									1
{131}										0
{137}										0
{139}			1							1
{149}										0
{151}										0
{157}										0
{163}	1								1	2
{167}										0
{173}										0
{179}										0
{181}	1									1
{191}										0
{193}										0
{197}										0
{199}	1	1	1							3
{211}			1	1						2
{223}										0
{227}										0
{229}			1							1

Table A.13: Old imprimitive nonics where S contains 2 primes.

S	T_2	T_4	T_5	T_8	Total
{2,3}		8	1	22	31
{2,5}					0
{3,5}		5	1	4	10
{2,7}					0
{3,7}	1	20	1	4	26
{5,7}		1			1
{2,11}				1	1
{3,11}		6	1	9	16

continued on next page

Table A.13: Old imprimitive nonics with $|S| = 2$ (*cont.)*

S	T_2	T_4	T_5	T_8	Total
{5,11}					0
{7,11}					0
{2,13}		2		1	3
{3,13}	1	32	2	16	51
{5,13}					0
{7,13}	1				1
{11,13}		1			1

Table A.14: New imprimitive nonics where S contains 2 primes.

S	T_1	T_3	T_6	T_{10}	T_{11}	T_{12}	T_{13}	T_{18}	T_{20}	T_{21}	T_{22}	T_{24}	T_{25}	T_{28}	T_{29}	T_{30}	T_{31}	Total
{2,3}	1	6		22	6	12	6	80	18	54	18	321	4	28	45	232	616	1469
{2,5}																1		1
{3,5}	1	4		17	4	12	4	8	12	54	12	48			1	40	5	222
{2,7}																		0
{3,7}	3	4	3	41	16		16	8	72		48	48			4	40	5	308
{5,7}				1														1
{2,11}																2	2	4
{3,11}	1	4		18	4	12	4	48	12	54	12	189			15	93	39	505
{5,11}																		0
{7,11}																		0
{2,13}				2												2	3	7
{3,13}	3	6	3	66	24	36	24	32	144	108	72	180			4	40	14	756
{5,13}													1					1
{7,13}																		0
{11,13}																1		1

Table A.15: All nonics from Table A.12.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^9-3x^6-6x^3-1$	-3^{19}	(3,3)	T_4	1	C_1
x^9-3x^3-1	-3^{21}	(3,3)	T_{13}	1	C_1
$x^9-6x^6+12x^3+1$	3^{22}	(1,4)	T_{11}	1	C_1
$x^9-9x^7+27x^5-30x^3+9x-1$	3^{22}	(9,0)	T_1	1	C_1
$x^9-3x^6-9x^3+3$	-3^{23}	(3,3)	T_{22}	1	C_1
$x^9-6x^6+9x^3-3$	-3^{23}	(3,3)	T_{22}	1	C_1
x^9-3x^6+3	-3^{23}	(3,3)	T_{22}	1	C_1
$x^9-9x^7-3x^6+27x^5+18x^4-15x^3-27x^2-36x-4$	-3^{25}	(3,3)	T_{20}	1	C_1
$x^9-9x^7-3x^6+27x^5+18x^4-24x^3-27x^2-9x+23$	-3^{25}	(3,3)	T_{20}	1	C_1
$x^9-9x^7-6x^6+27x^5+36x^4-24x^3-54x^2-9x+22$	-3^{25}	(3,3)	T_{20}	1	C_1
$x^9-9x^6+27x^3-3$	3^{26}	(1,4)	T_3	1	C_1
x^9-3	3^{26}	(1,4)	T_{10}	1	C_1
$x^9-9x^6+27x^3-24$	3^{26}	(1,4)	T_{10}	1	C_1
$x^9-x^8-8x^7+7x^6+21x^5-15x^4-20x^3+10x^2+5x-1$	19^8	(9,0)	T_1	1	C_1
$x^9-x^7-2x^6+3x^5+x^4+2x^3-x^2+x-3$	31^6	(1,4)	T_{10}	1	C_1
$x^9-3x^8+4x^7-10x^6+5x^5+19x^4-49x^3+131x^2-153x+47$	-31^7	(3,3)	T_4	1	C_1
$x^9-x^8-16x^7+11x^6+66x^5-32x^4-73x^3+7x^2+7x-1$	37^8	(9,0)	T_1	1	C_1
$x^9-x^8-32x^7+11x^6+278x^5+34x^4-427x^3-150x^2-8x+1$	73^8	(9,0)	T_1	1	C_1
$x^9-x^8-48x^7+73x^6+660x^5-1454x^4-2149x^3+8350x^2-7432x+2008$	109^8	(9,0)	T_1	1	C_1
$x^9-x^8-56x^7+118x^6+573x^5-1249x^4-1582x^3+2700x^2+1576x-32$	127^8	(9,0)	T_1	1	C_1
$x^9-x^8-80x^7-53x^6+1668x^5+3314x^4-4261x^3-10795x^2-2933x+1949$	181^8	(9,0)	T_1	1	C_1
$x^9-x^8-3x^6+3x^3+3x^2+5x+1$	199^4	(1,4)	T_3	1	C_1
$x^9-3x^8+4x^7+19x^6-109x^5+1761x^4-12265x^3+9172x^2+7660x+13123$	-199^7	(3,3)	T_4	1	C_1
$x^9-x^8-88x^7+325x^6+775x^5-3447x^4-1602x^3+7354x^2-3333x-121$	199^8	(9,0)	T_1	1	C_1
$x^9-2x^8-17x^7+36x^6+90x^5-143x^4-262x^3-179x^2+1441x-672$	211^6	(1,4)	T_{10}	1	C_1

continued on next page

TABLE A.15: All nonics from Table A.12. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^9 - 4x^8 + 10x^7 + 134x^6 - 337x^5 - 404x^4 - 1074x^3 + 6283x^2 - 6079x + 1699$	-211^7	(3,3)	T_4	1	C_1
$x^9 - x^8 - 78x^7 + 112x^6 + 1748x^5 - 2896x^4 - 12661x^3 + 21649x^2 + 25102x - 40976$	229^7	(9,0)	T_4	1	C_1
$x^9 - x^8 + 2x^7 + 128x^6 + 459x^5 + 745x^4 + 578x^3 - 529x^2 - 885x + 431$	-139^7	(3,3)	T_4	4	C_2C_2
$x^9 - 3x^8 + 31x^7 - 35x^6 + 191x^5 + 117x^4 - 40x^3 - 56x^2 - 251x - 155$	-163^7	(3,3)	T_{28}	4	C_2C_2
$x^9 - x^8 - 72x^7 + 73x^6 + 1482x^5 - 1034x^4 - 9637x^3 + 1173x^2 + 10087x - 853$	163^8	(9,0)	T_1	4	C_2C_2

Table A.16: All nonics from Tables A.13 and A.14 having class number $h \geq 8$.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
x^9+66x^3-33	$3^{20}11^8$	(1,4)	T_{21}	8	C_4C_2
$x^9-135x^6-675x^4+495x^3-9315x^2-41040x-68880$	$3^{26}5^8$	(1,4)	T_{30}	8	$C_2C_2C_2$
$x^9-6x^6+45x^5-72x^4+54x^3-18x^2+8$	$2^{16}3^{18}$	(1,4)	T_{30}	9	C_9
$x^9-9x^7-18x^6-9x^5-36x^4-75x^3-90x^2+36x-8$	$2^{16}3^{18}$	(1,4)	T_{30}	9	C_9
$x^9-18x^7-12x^6+99x^5+108x^4-132x^3-72x^2+126x+80$	$2^{16}3^{18}$	(1,4)	T_{30}	9	C_9
$x^9+9x^7-18x^6+81x^5-72x^4+51x^3+54x^2-54x+28$	$2^{12}3^{22}$	(1,4)	T_3	9	C_9
$x^9-9x^7-18x^6+27x^5+108x^4+33x^3-162x^2-180x-568$	$2^{14}3^{22}$	(1,4)	T_{30}	9	C_9
$x^9+18x^7-18x^6+108x^5-216x^4+312x^3-648x^2+576x-64$	$2^{16}3^{22}$	(1,4)	T_{30}	9	C_9
$x^9-18x^7-36x^6+81x^5+468x^4+708x^3-432x^2-2592x-2240$	$2^{16}3^{22}$	(1,4)	T_{30}	9	C_3C_3
$x^9-18x^6+54x^5-72x^4+105x^3-270x^2+396x-352$	$3^{22}11^4$	(1,4)	T_3	9	C_9
$x^9-9x^7+27x^5-39x^3+36x-17$	$3^{22}11^4$	(1,4)	T_{30}	9	C_9
$x^9-24x^6+72x^5-108x^4+45x^3-9x^2-9x-1$	$3^{18}11^6$	(1,4)	T_{30}	9	C_9
$x^9-18x^7-27x^6+81x^5+441x^4+1527x^3+1188x^2-1188x-1232$	$3^{22}11^6$	(1,4)	T_{30}	9	C_3C_3
$x^9-18x^7-27x^6+81x^5+441x^4+1329x^3-5940x^2+3564x-2024$	$3^{22}11^6$	(1,4)	T_{30}	9	C_9
$x^9+9x^7-9x^6+27x^5-54x^4-297x^3-81x^2+81x-27$	$-3^{15}13^7$	(3,3)	T_{18}	9	C_3C_3
$x^9-39x^6-156x^3-169$	$3^{18}13^7$	(1,4)	T_{24}	9	C_3C_3
$x^9+9x^7-69x^6+27x^5-765x^4+795x^3-2727x^2+2304x+937$	$-3^{19}13^7$	(3,3)	T_{18}	9	C_3C_3
$x^9+27x^7-9x^6+243x^5-162x^4+756x^3-729x^2+243x-2835$	$3^{20}13^7$	(1,4)	T_{24}	9	C_3C_3
$x^9+36x^7-33x^6+432x^5-441x^4+1857x^3-891x^2+1782x+1932$	$3^{20}13^7$	(1,4)	T_{24}	9	C_3C_3
$x^9-27x^7-72x^6+243x^5+1296x^4-54x^3-5832x^2-6075x-2592$	$3^{20}13^7$	(1,4)	T_{24}	9	C_3C_3
$x^9-351x^6+30888x^3+1521$	$3^{26}13^7$	(1,4)	T_{24}	9	C_3C_3
$x^9+3159x^3-32448$	$3^{26}13^7$	(1,4)	T_{24}	9	C_3C_3
$x^9-81x^7-45x^6+2187x^5+4536x^4+8019x^3-26487x^2-44550x-28764$	$3^{26}13^7$	(1,4)	T_{24}	9	C_9
$x^9+27x^7-9x^6-810x^5-1566x^4+8127x^3+44550x^2+77463x+32421$	$3^{26}13^7$	(1,4)	T_{24}	9	C_9
$x^9+81x^7-225x^6+2187x^5-4428x^4+12573x^3+31833x^2-90882x+156300$	$3^{26}13^7$	(1,4)	T_{24}	9	C_9

continued on next page

Table A.16: All nonics from Tables A.13 and A.14 having class number $h \geq 8$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^9 - 9x^7 - 12x^6 + 27x^5 + 18x^4 + 255x^3 - 594x^2 + 720x - 700$	$2^{10}3^{25}$	(1,4)	T_{31}	10	C_{10}
$x^9 - 66x^6 - 1331$	$3^{21}11^7$	(1,4)	T_{18}	12	C_{12}
$x^9 + 726x^3 - 1331$	$3^{21}11^7$	(1,4)	T_{18}	12	C_{12}
$x^9 - 9x^7 - 111x^6 + 27x^5 + 666x^4 + 2676x^3 - 999x^2 - 8109x + 6911$	$-3^{19}13^7$	(3,3)	T_4	12	C_6C_2
$x^9 - 42x^6 + 702x^4 + 2343x^3 + 3159x^2 - 6669x - 23687$	$3^{22}13^6$	(1,4)	T_{30}	12	C_6C_2
$x^9 - 30x^6 - 51x^3 - 64$	$3^{22}13^6$	(1,4)	T_{11}	12	C_6C_2
$x^9 - 117x^3 - 117$	$-3^{23}13^8$	(3,3)	T_{22}	12	C_6C_2
$x^9 + 27x^7 - 126x^6 + 243x^5 + 540x^4 - 5094x^3 + 1377x^2 - 120501x - 427467$	$3^{26}13^7$	(1,4)	T_{31}	12	C_6C_2
$x^9 - 234x^6 - 3510x^3 - 267501$	$3^{26}13^8$	(1,4)	T_{10}	12	C_6C_2
$x^9 - 117x^6 - 1053x^4 + 3159x^3 - 1053x^2 + 40716x - 86736$	$3^{26}13^8$	(1,4)	T_{30}	12	C_6C_2
$x^9 - 1053$	$3^{26}13^8$	(1,4)	T_{10}	12	C_6C_2
$x^9 - 84x^6 + 315x^5 - 1008x^4 + 2037x^3 - 1827x^2 + 630x - 112$	$3^{22}7^8$	(1,4)	T_{30}	12	C_6C_2
$x^9 + 27x^7 - 18x^6 + 243x^5 - 324x^4 + 837x^3 - 1458x^2 + 972x - 69$	$3^{26}7^6$	(1,4)	T_{30}	12	C_6C_2
$x^9 - 63x^7 - 210x^6 - 378x^5 - 1008x^4 - 231x^3 - 1890x^2 + 1071x - 364$	$-3^{25}7^8$	(3,3)	T_{20}	12	C_6C_2
$x^9 + 756x^3 - 63$	$3^{26}7^8$	(1,4)	T_{10}	12	C_6C_2
$x^9 - 63x^6 + 567x^5 - 1701x^4 + 4095x^3 - 2268x^2 + 756x + 12264$	$3^{26}7^8$	(1,4)	T_{30}	12	C_6C_2
$x^9 - 39x^6 + 351x^5 - 1053x^4 + 741x^3 + 1404x^2 - 1404x - 208$	$-3^{19}13^8$	(3,3)	T_{29}	18	C_6C_3
$x^9 - 63x^7 - 33x^6 + 1323x^5 + 1386x^4 - 10536x^3 - 14553x^2 + 26775x + 42232$	$-3^{25}13^6$	(3,3)	T_{29}	18	C_{18}
$x^9 - 27x^7 - 6x^6 + 243x^5 - 594x^4 + 2208x^3 - 2592x^2 + 6912x - 11552$	$3^{24}13^7$	(1,4)	T_{24}	18	C_6C_3
$x^9 - 27x^7 - 6x^6 + 243x^5 + 459x^4 + 921x^3 + 1620x^2 + 2700x + 2176$	$3^{24}13^7$	(1,4)	T_{24}	18	C_6C_3
$x^9 - 9x^7 - 6x^6 + 27x^5 + 36x^4 - 15x^3 - 54x^2 - 36x + 31$	$-3^{25}13^7$	(3,3)	T_{31}	18	C_{18}
$x^9 - 117x^7 - 39x^6 + 4563x^5 + 3042x^4 - 55770x^3 - 59319x^2 - 138411x - 115258$	$-3^{25}13^8$	(3,3)	T_{29}	18	C_{18}
$x^9 - 117x^7 - 78x^6 + 351x^5 + 1521x^4 - 2652x^3 + 2457x^2 - 4680x - 4199$	$-3^{25}13^8$	(3,3)	T_{29}	18	C_{18}
$x^9 - 42x^6 - 126x^5 + 189x^4 + 273x^3 - 1071x^2 + 112$	$-3^{21}7^8$	(3,3)	T_{29}	18	C_{18}
$x^9 - 756x^4 - 3969x^3 - 4032$	$-3^{25}7^8$	(3,3)	T_{29}	18	C_{18}

continued on next page

TABLE A.16: All nonics from Tables A.13 and A.14 having class number $h \geq 8$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^9 - 63x^7 - 42x^6 + 756x^5 + 1008x^4 - 2688x^3 - 6048x^2 - 4032x - 896$	$-3^{25}7^8$	(3,3)	T_{29}	18	C_{18}
$x^9 - 117x^7 - 312x^6 + 1404x^5 + 3627x^4 - 6864x^3 - 11232x^2 + 15327x - 7241$	$-3^{25}13^8$	(3,3)	T_{20}	24	$C_6C_2C_2$
$x^9 - 27x^7 + 243x^5 - 729x^3 - 3969$	$3^{26}7^6$	(1,4)	T_{30}	24	$C_6C_2C_2$
$x^9 - 1701x^3 - 108864$	$3^{26}7^8$	(1,4)	T_{10}	24	$C_{12}C_2$
$x^9 - 63x^6 + 2646x^4 + 2646x^3 - 23814x^2 - 103194x + 20727$	$-3^{25}7^8$	(3,3)	T_{20}	42	C_{42}
$x^9 - 234x^6 + 2106x^4 + 3159x^3 - 24219x^2 + 21411x - 18213$	$3^{26}13^8$	(1,4)	T_{30}	48	$C_6C_2C_2C_2$
$x^9 + 9x^7 - 9x^6 + 27x^5 - 54x^4 + 54x^3 - 81x^2 + 81x - 339$	$3^{24}13^7$	(1,4)	T_{24}	54	$C_{18}C_3$

A.4. Imprimitive Decic Tables

We now provide tables for imprimitive fields of degree 10. We partition the imprimitive decics into 2 groups, those with a quintic subfield and those with a quadratic subfield. For those cases having 2 primes and a quintic subfield, the fields were further partitioned into new and old fields.

Tables A.17, A.18, A.19 A.20, A.21, and A.22 give numbers of each type of field for various sets S. In addition, Table A.21 sorts the data by quadratic subfield K. As in previous cases, if a column does not exist for a specific type of field then that means that no fields of that type were found for all cases in that table. Finally, note that Table A.22 is not complete, but is guaranteed to contain every field satisfying $\nu_2(d_L) \leq 27$.

Tables A.23, A.24, and A.25 give specific field data, ordered by increasing class number. In the interest of saving space, Table A.24 only lists those fields having a class number greater than or equal to 32.

TABLE A.17: Decics with a quintic subfield ($|S| = 1$).

S	T_1	T_2	T_4	T_{12}	T_{24}	T_{25}	T_{37}	T_{38}	Total
{2}									0
{3}									0
{5}	1		2						3
{7}									0
{11}	1								1
{13}									0
{17}									0
{19}									0
{23}									0
{29}									0
{31}	1								1
{37}									0
{41}	1								1
{43}									0
{47}		1							1
{53}									0
{59}									0
{61}	1								1
{67}									0
{71}	1								1
{73}									0
{79}		1							1
{83}									0

continued on next page

TABLE A.17: Decics with a quintic subfield ($|S| = 1$). *(cont.)*

S	T_1	T_2	T_4	T_{12}	T_{24}	T_{25}	T_{37}	T_{38}	Total
{89}									0
{97}									0
{101}	1		1	1			1	1	5
{103}		1							1
{107}									0
{109}									0
{113}									0
{127}		1							1
{131}	1	1							2
{137}									0
{139}									0
{149}									0
{151}	1			1					2
{157}			1		1	1			3
{163}									0
{167}									0
{173}			1		1	1			3
{179}		1							1
{181}	1		1						2
{191}	1								1
{193}									0
{197}			1						1
{199}									0
{211}	1								1
{223}									0
{227}		1							1
{229}									0

TABLE A.18: Old decics with a quintic subfield ($|S| = 2$).

S	T_1	T_2	T_3	T_4	T_5	T_{11}	T_{12}	T_{22}	Total
{2,3}				1	6		5	30	42
{2,5}	7	4	24	19	114	35	38	228	469
{3,5}	3	2	4	7	14	18	22	44	114
{2,7}							2	12	14

continued on next page

Table A.18: Old decics with a quintic subfield ($|S| = 2$). (*cont.)*

S	T_1	T_2	T_3	T_4	T_5	T_{11}	T_{12}	T_{22}	Total
{3,7}									0
{5,7}	3	2	4	7	14		4	8	42
{2,11}	7	1	6	1	6		2	12	35
{3,11}	3					6			9
{7,11}	3	1	2				1	2	9
{2,13}				6	36		4	24	70
{3,13}									0
{7,13}				1	2				3
{11,13}	3	1	2						6
{2,17}						7	3	18	28
{3,17}				1	2	3	1	2	9
{7,17}		1	2						3
{11,17}	3								3
{13,17}				1	2				3
{2,19}		1	6	1	6	7	2	12	35
{3,19}						9	4	8	21
{7,19}		1	2						3
{11,19}	3	2	4				1	2	12
{13,19}							1	2	3
{17,19}							1	2	3
{2,23}				1	6		5	30	42
{3,23}						3			3
{7,23}							1	2	3
{11,23}	3						1	2	6
{13,23}									0
{17,23}				1	2				3
{19,23}		1	2				2	4	9
{2,29}		1	6	2	12	14	6	36	77
{3,29}		1	2	1	2	9			15
{7,29}							2	4	6
{11,29}	3	2	4						9
{13,29}				1	2	3	2	4	12
{17,29}				2	4	6	3	6	21
{19,29}		1	2	1	2				6
{23,29}						6	1	2	9

Table A.19: New decics with a quintic subfield ($|S| = 2$).

S	T_8	T_{14}	T_{15}	T_{16}	T_{23}	T_{24}	T_{25}	T_{29}	T_{34}	T_{36}	T_{37}	T_{38}	T_{39}	Total
{2,3}						7	7	42			91	91	546	784
{2,5}	3	21	60	60	360	173	173	1038	35	245	450	450	2700	5768
{3,5}											8	8	16	32
{2,7}											30	30	180	240
{3,7}														0
{5,7}	3	9				1	1	2			1	1	2	20
{2,11}	3	21	15	15	90	15	15	90			46	46	276	632
{3,11}														0
{7,11}											1	1	2	4
{2,13}						90	90	540			84	84	504	1392
{3,13}														0
{7,13}														0
{11,13}			3	3	6									12
{2,17}									15	105	61	61	366	608
{3,17}									1	3	1	1	2	8
{7,17}			3	3	6									12
{11,17}														0
{13,17}						1	1	2						4
{2,19}			15	15	90	15	15	90	7	49	46	46	276	664
{3,19}											3	3	6	12
{7,19}														0
{11,19}														0
{13,19}														0
{17,19}											3	3	6	12
{2,23}						31	31	186			107	107	642	1104
{3,23}									1	3				4
{7,23}											1	1	2	4
{11,23}	3	9												12
{13,23}														0
{17,23}						1	1	2						4
{19,23}											1	1	2	4
{2,29}			15	15	90	22	22	132	22	154	138	138	828	1576
{3,29}									1	3				4
{7,29}											1	1	2	4
{11,29}			3	3	6									12
{13,29}						1	1	2			4	4	8	20
{17,29}						1	1	2			1	1	2	8

continued on next page

Table A.19: New decics with a quintic subfield ($|S| = 2$). (*cont.)*

S	T_8	T_{14}	T_{15}	T_{16}	T_{23}	T_{24}	T_{25}	T_{29}	T_{34}	T_{36}	T_{37}	T_{38}	T_{39}	Total
{19,29}						3	3	6						12
{23,29}											3	3	6	12

Table A.20: Decics with a quadratic subfield ($|S| = 1$).

S	T_1	T_2	T_4	T_{10}	Total
{2}					0
{3}					0
{5}	1		2	2	5
{7}					0
{11}	1				1
{13}					0
{17}					0
{19}					0
{23}					0
{29}					0
{31}	1				1
{37}					0
{41}	1				1
{43}					0
{47}		1			1

Table A.21: Decics with a quadratic subfield ($|S| = 2$).

S	K	T_1	T_2	T_3	T_5	T_6	T_{11}	T_{22}	T_{40}	T_{41}	T_{43}	Total
{2,3}	$\mathbb{Q}(\sqrt{-3})$				1			5	1	2	3	12
{2,3}	$\mathbb{Q}(\sqrt{-1})$				1			5	0	2	6	14
{3,7}	$\mathbb{Q}(\sqrt{-3})$											0
{3,7}	$\mathbb{Q}(\sqrt{-7})$											0
{3,7}	$\mathbb{Q}(\sqrt{21})$											0
{3,11}	$\mathbb{Q}(\sqrt{-3})$	1					2					3
{3,11}	$\mathbb{Q}(\sqrt{-11})$	1					2					3
{3,11}	$\mathbb{Q}(\sqrt{33})$	1					2					3

continued on next page

Table A.21: Decics with a quadratic subfield ($|S| = 2$). (*cont.)*

S	K	T_1	T_2	T_3	T_5	T_6	T_{11}	T_{22}	T_{40}	T_{41}	T_{43}	Total
$\{7,11\}$	$\mathbb{Q}(\sqrt{-7})$	1	1			2		1				5
$\{7,11\}$	$\mathbb{Q}(\sqrt{-11})$	1		1				1				3

Table A.22: All decics unramified outside $S = \{2, 3\}$, containing $K = \mathbb{Q}(\sqrt{2})$, and such that $\nu_2(d_L) \leq 27$.

S	K	T_4	T_{12}	T_{22}	T_{40}	T_{43}	Total
$\{2,3\}$	$\mathbb{Q}(\sqrt{2})$	1	2	3	2	3	11

TABLE A.23: All decics from Tables A.17 and A.20.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^{10}-x^5-1$	5^{15}	(2,4)	T_4	1	C_1
$x^{10}-10x^8+35x^6-x^5-50x^4+5x^3+25x^2-5x-1$	5^{17}	(10,0)	T_1	1	C_1
$x^{10}-5x^5-5$	5^{19}	(2,4)	T_{10}	1	C_1
$x^{10}-5$	5^{19}	(2,4)	T_4	1	C_1
$x^{10}-5x^5+5$	5^{19}	(2,4)	T_{10}	1	C_1
$x^{10}-x^9+x^8-x^7+x^6-x^5+x^4-x^3+x^2-x+1$	-11^9	(0,5)	T_1	1	C_1
$x^{10}-x^9-18x^8+13x^7+91x^6-47x^5-143x^4+7x^3+72x^2+23x+1$	41^9	(10,0)	T_1	1	C_1
$x^{10}-x^9+6x^8-3x^7+11x^6-3x^5+11x^4-3x^3+6x^2-x+1$	-47^5	(0,5)	T_2	1	C_1
$x^{10}-x^9-27x^8+56x^7+161x^6-500x^5+x^4+1023x^3-916x^2+202x-13$	61^9	(10,0)	T_1	1	C_1
$x^{10}-2x^9+3x^8-7x^7+x^6+2x^5+19x^4-25x^3+21x^2-5x+1$	-79^5	(0,5)	T_2	1	C_1
$x^{10}-4x^9-5x^8+29x^7+13x^6-59x^5-13x^4+29x^3+5x^2-4x-1$	101^7	(2,4)	T_{12}	1	C_1
$x^{10}-5x^9+3x^8+18x^7-12x^6-48x^5+21x^4+69x^3+6x^2-53x-19$	101^7	(2,4)	T_4	1	C_1
$x^{10}-4x^9+3x^8+2x^7+10x^6-27x^5+x^4+41x^3-59x^2+72x-44$	101^7	(2,4)	T_{38}	1	C_1
$x^{10}-x^9-45x^8+12x^7+614x^6+399x^5-2937x^4-3927x^3+3176x^2+7776x+3433$	101^9	(10,0)	T_1	1	C_1
$x^{10}-2x^9+3x^8+x^7-15x^6+22x^5+9x^4-65x^3+77x^2-39x+9$	-103^5	(0,5)	T_2	1	C_1
$x^{10}-5x^9+18x^8-42x^7+76x^6-102x^5+99x^4-67x^3+22x^2+9$	-127^5	(0,5)	T_2	1	C_1
$x^{10}-4x^9+4x^8-4x^7+9x^6-6x^5+12x^4-2x^3+41x^2-2x+4$	-131^5	(0,5)	T_2	1	C_1
$x^{10}-5x^9+5x^8+8x^7-64x^6+153x^5-31x^4-437x^3+673x^2-326x+104$	157^7	(2,4)	T_{25}	1	C_1
$x^{10}-5x^9-3x^8+42x^7+30x^6-258x^5+143x^4+203x^3-360x^2+207x-351$	157^7	(2,4)	T_4	1	C_1
$x^{10}-8x^8+26x^6-37x^4+17x^2-4$	173^6	(2,4)	T_{24}	1	C_1
$x^{10}-x^9+11x^8+4x^7+45x^6+49x^5+131x^4+148x^3+156x^2+144x+64$	-179^5	(0,5)	T_2	1	C_1
$x^{10}-x^9-7x^8+3x^7+18x^6+81x^5-53x^4-358x^3-59x^2+600x+400$	181^7	(2,4)	T_4	1	C_1
$x^{10}-x^9-81x^8+94x^7+2418x^6-3121x^5-31973x^4+43245x^3+170860x^2-209252x-201337$	181^9	(10,0)	T_1	1	C_1
$x^{10}-5x^9-5x^8+50x^7-37x^6-85x^5+256x^4-302x^3-35x^2+162x-311$	197^7	(2,4)	T_4	1	C_1
$x^{10}-2x^9+5x^8-4x^7-9x^6+28x^5-41x^4+30x^3+99x^2+16x+113$	-227^5	(0,5)	T_2	1	C_1
$x^{10}+13x^8-7x^7+53x^6-33x^5+19x^4+536x^3-149x^2+2750x-2164$	101^8	(2,4)	T_{37}	2	C_2
$x^{10}-4x^9-7x^8+77x^7-490x^6+2282x^5-5873x^4+9219x^3-11162x^2+10642x-4721$	157^8	(2,4)	T_{24}	2	C_2
$x^{10}-x^9+2x^8+16x^7-9x^6+11x^5+43x^4-6x^3+63x^2-20x+25$	-31^9	(0,5)	T_1	3	C_3

continued on next page

TABLE A.23: All decics from Tables A.17 and A.20. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^{10} - 2x^9 - 6x^8 + 31x^7 - 41x^6 - 103x^5 + 446x^4 - 247x^3 - 1049x^2 + 1695x - 729$	173^7	(2,4)	T_{25}	4	C_4
$x^{10} - 5x^9 - 3x^8 + 42x^7 - 74x^6 + 54x^5 - 39x^4 + 47x^3 - 16x^2 - 7x - 1$	173^7	(2,4)	T_4	4	C_2C_2
$x^{10} - x^9 + 4x^8 - 20x^7 - 103x^6 - 141x^5 + 207x^4 + 1254x^3 + 2635x^2 + 4020x + 3737$	-71^9	(0,5)	T_1	7	C_7
$x^{10} - 3x^9 + 13x^8 - 11x^7 + 41x^6 - 44x^5 + 51x^4 - 71x^3 + 47x^2 - 40x + 25$	-151^7	(0,5)	T_{12}	7	C_7
$x^{10} - x^9 + 7x^8 - 63x^7 + 237x^6 - 783x^5 + 7565x^4 - 21935x^3 + 39574x^2 - 36034x + 18289$	-131^9	(0,5)	T_1	25	C_{25}
$x^{10} - x^9 + 11x^8 - 17x^7 + 1116x^6 - 826x^5 + 6434x^4 + 13908x^3 + 196774x^2 + 64432x + 1107131$	-211^9	(0,5)	T_1	123	C_{123}
$x^{10} - x^9 + 10x^8 + 252x^7 - 216x^6 - 3244x^5 + 17715x^4 - 24287x^3 + 16260x^2 - 5200x + 625$	-191^9	(0,5)	T_1	1573	$C_{143}C_{11}$
$x^{10} - x^9 + 8x^8 + 18x^7 + 397x^6 + 351x^5 + 4010x^4 + 720x^3 + 4352x^2 - 11264x + 292352$	-151^9	(0,5)	T_1	1967	C_{1967}

TABLE A.24: All decics from Tables A.18 and A.19 having class number $h \geq 32$.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^{10}+26x^8+182x^6+572x^4+1014x^2+676$	$-2^{30}13^8$	(0,5)	T_{39}	32	$C_{16}C_2$
$x^{10}+30x^8+308x^6+1224x^4+1436x^2+392$	$-2^{33}13^8$	(0,5)	T_{29}	32	$C_{16}C_2$
$x^{10}+29x^8+58x^6-406x^4+2001x^2+10469$	$-2^{22}29^9$	(0,5)	T_{39}	32	$C_8C_2C_2$
$x^{10}+29x^8+232x^6+464x^4+1856$	$-2^{24}29^9$	(0,5)	T_{39}	32	$C_8C_2C_2$
$x^{10}+20x^8+130x^6+340x^4+335x^2+72$	$-2^{33}5^{12}$	(0,5)	T_{29}	32	$C_{16}C_2$
$x^{10}+30x^8-10x^7+165x^6-231x^5+835x^3+255x^2+505x+2699$	$-5^{17}7^5$	(0,5)	T_1	32	C_2^5
$x^{10}+28x^8+272x^6+1216x^4+3496x^2+5472$	$-2^{31}19^7$	(0,5)	T_{38}	34	C_{34}
$x^{10}+38x^8+342x^6+1596x^4+4313x^2+6422$	$-2^{21}19^9$	(0,5)	T_{11}	36	C_6C_6
$x^{10}+29x^8+290x^6+290x^4+145x^2+261$	$-2^{16}29^9$	(0,5)	T_{11}	36	C_6C_6
$x^{10}+14x^8+90x^6+252x^4+898x^2+1352$	$-2^{23}29^8$	(0,5)	T_{36}	36	$C_{12}C_3$
$x^{10}-2x^9+21x^8-31x^7+212x^6-253x^5+1249x^4-1309x^3+4949x^2-4122x+6444$	$-23^7 29^5$	(0,5)	T_{12}	36	C_{36}
$x^{10}-50x^6-80x^5+250x^4+1000x^3+1925x^2+2600x+1690$	$-2^{17}5^{19}$	(0,5)	T_{22}	36	$C_{18}C_2$
$x^{10}+25x^8+200x^6-40x^5+2500x^4+2000x^3+10000x^2-4000x+400$	$-2^{18}5^{19}$	(0,5)	T_{12}	36	$C_{18}C_2$
$x^{10}+5x^8+160x^6+760x^4+880x^2+16$	$-2^{22}5^{18}$	(0,5)	T_{39}	36	$C_{18}C_2$
$x^{10}-10x^8+800x^6+22400x^4+37600x^2+2880$	$-2^{34}5^{17}$	(0,5)	T_{39}	36	$C_{18}C_2$
$x^{10}-x^9+45x^8-73x^7+476x^6-489x^5+2760x^4+823x^3+3121x^2+8533x+5720$	$-19^7 23^8$	(0,5)	T_{39}	40	$C_{20}C_2$
$x^{10}-14x^8+74x^6-172x^4+144x^2+32$	$-2^{25}11^8$	(0,5)	T_{16}	40	C_{40}
$x^{10}+33x^6+198x^4+110x^2+44$	$-2^{24}11^9$	(0,5)	T_{23}	40	$C_{10}C_2C_2$
$x^{10}-22x^6+704x^4+4400x^2+1408$	$-2^{25}11^9$	(0,5)	T_{23}	40	$C_{20}C_2$
$x^{10}+22x^8+110x^6-308x^4-704x^2+1408$	$-2^{25}11^9$	(0,5)	T_{23}	40	$C_{20}C_2$
$x^{10}-5x^8+200x^4-225x^2+605$	$-2^{14}5^{17}$	(0,5)	T_{23}	40	$C_{20}C_2$
$x^{10}-5x^8-25x^6+225x^4-600x^2+980$	$-2^{14}5^{17}$	(0,5)	T_{23}	40	$C_{20}C_2$
$x^{10}+5x^8-15x^6-115x^4+80x^2+576$	$-2^{18}5^{16}$	(0,5)	T_{16}	40	$C_{20}C_2$
$x^{10}+5x^8+25x^6+25x^4+20$	$-2^{18}5^{17}$	(0,5)	T_{23}	40	$C_{10}C_2C_2$
$x^{10}+110x^6+140x^4+160x^2+32$	$-2^{21}5^{16}$	(0,5)	T_{23}	40	C_{40}
$x^{10}+10x^8+50x^6+200x^4+800x^2+640$	$-2^{19}5^{17}$	(0,5)	T_{23}	40	$C_{10}C_2C_2$
$x^{10}+10x^8-25x^6-250x^4+1450x^2+640$	$-2^{19}5^{17}$	(0,5)	T_{23}	40	$C_{10}C_2C_2$
$x^{10}-5x^8+100x^6-350x^4+1800x^2+6480$	$-2^{20}5^{17}$	(0,5)	T_{23}	40	$C_{20}C_2$

continued on next page

TABLE A.24: All decics from Tables A.18 and A.19 having class number $h \geq 32$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^{10} - 10x^8 + 1600x^2 - 640$	$2^{21}5^{17}$	(2,4)	T_{23}	40	$C_{20}C_2$
$x^{10} + 38x^8 + 10944x^4 + 92416x^2 + 184832$	$-2^{33}19^8$	(0,5)	T_{39}	44	$C_{22}C_2$
$x^{10} + 20x^6 + 160x^4 + 220x^2 + 32$	$-2^{33}5^{12}$	(0,5)	T_{38}	44	$C_{22}C_2$
$x^{10} + 30x^8 + 310x^6 + 1260x^4 + 1480x^2 + 16$	$-2^{24}5^{18}$	(0,5)	T_{39}	44	$C_{22}C_2$
$x^{10} + 40x^6 + 80x^4 + 560x^2 + 576$	$-2^{20}5^{16}$	(0,5)	T_{36}	45	$C_{15}C_3$
$x^{10} + 30x^8 + 310x^6 + 1260x^4 + 1580x^2 + 576$	$-2^{18}5^{18}$	(0,5)	T_{29}	45	C_{45}
$x^{10} - 3x^9 + 24x^8 - 52x^7 + 310x^6 - 484x^5 + 2334x^4 - 2373x^3 + 10496x^2 - 5129x + 22793$	$-11^8 23^5$	(0,5)	T_1	48	$C_6C_2^3$
$x^{10} + 26x^8 + 208x^6 + 832x^4 + 2704x^2 + 5408$	$-2^{29}13^8$	(0,5)	T_{39}	48	$C_{24}C_2$
$x^{10} - x^9 + 34x^8 - 34x^7 + 430x^6 - 430x^5 + 2509x^4 - 2509x^3 + 6964x^2 - 6964x + 9637$	$-11^9 13^5$	(0,5)	T_1	50	C_{50}
$x^{10} - 2x^9 + 4x^8 + 4x^7 + 141x^6 + 215x^5 + 776x^4 + 209x^3 + 71x^2 - 803x + 1130$	$-19^5 29^7$	(0,5)	T_5	52	$C_{26}C_2$
$x^{10} - 3x^9 + 19x^8 - 40x^7 + 210x^6 - 320x^5 + 1364x^4 - 1353x^3 + 5467x^2 - 2585x + 10879$	$-11^8 19^5$	(0,5)	T_1	55	C_{55}
$x^{10} + 29x^8 + 261x^6 + 899x^4 + 2088x^2 + 3364$	$-2^{20}29^8$	(0,5)	T_{39}	56	$C_{14}C_2C_2$
$x^{10} + 50x^8 + 875x^6 + 6250x^4 + 15625x^2 + 1250$	$-2^{19}5^{18}$	(0,5)	T_5	56	C_{56}
$x^{10} - 2x^9 + 7x^8 + 24x^7 + 288x^6 + 1312x^5 + 3352x^4 + 7096x^3 + 10445x^2 + 7382x + 2235$	$-2^{27}13^9$	(0,5)	T_5	60	$C_{30}C_2$
$x^{10} + 29x^8 + 145x^6 + 609x^4 + 14384x^2 + 67048$	$-2^{21}29^9$	(0,5)	T_{39}	60	$C_{30}C_2$
$x^{10} + 10x^8 + 25x^6 - 100x^4 + 640$	$-2^{15}5^{17}$	(0,5)	T_{23}	60	$C_{30}C_2$
$x^{10} - 10x^8 + 40x^6 - 40x^4 - 10x^2 + 20$	$-2^{34}5^{11}$	(0,5)	T_{29}	60	$C_{30}C_2$
$x^{10} - 10x^8 + 55x^6 - 150x^4 + 415x^2 + 32$	$-2^{23}5^{16}$	(0,5)	T_{36}	60	C_{60}
$x^{10} + 50x^6 + 625x^2 - 1000$	$2^{21}5^{17}$	(2,4)	T_{11}	60	$C_{30}C_2$
$x^{10} + 10x^8 + 50x^6 + 550x^4 + 1575x^2 + 3240$	$-2^{23}5^{17}$	(0,5)	T_{36}	60	$C_{30}C_2$
$x^{10} - 10x^8 + 25x^6 - 50x^4 + 25x^2 - 40$	$2^{23}5^{17}$	(2,4)	T_{36}	60	$C_{30}C_2$
$x^{10} + 20x^8 + 300x^6 - 1000x^4 + 1000x^2 - 320$	$2^{24}5^{17}$	(2,4)	T_{36}	60	$C_{30}C_2$
$x^{10} - 50x^8 + 950x^6 - 8000x^4 + 23750x^2 + 18000$	$-2^{24}5^{17}$	(0,5)	T_{36}	60	$C_{30}C_2$
$x^{10} - 20x^8 + 300x^6 - 2600x^4 + 11800x^2 + 320$	$-2^{24}5^{17}$	(0,5)	T_{36}	60	$C_{30}C_2$
$x^{10} + 20x^8 + 100x^6 - 200x^4 - 600x^2 - 320$	$2^{24}5^{17}$	(2,4)	T_{36}	60	$C_{30}C_2$
$x^{10} + 10x^8 - 50x^6 + 100x^4 - 100x^2 + 40$	$-2^{25}5^{17}$	(0,5)	T_{36}	60	$C_{30}C_2$
$x^{10} - 10x^8 + 50x^6 - 100x^4 + 100x^2 - 40$	$2^{25}5^{17}$	(2,4)	T_{36}	60	$C_{30}C_2$
$x^{10} - 10x^8 + 100x^6 - 200x^4 + 100x^2 - 40$	$2^{25}5^{17}$	(2,4)	T_{36}	60	$C_{30}C_2$
$x^{10} + 10x^8 - 200x^4 + 300x^2 + 40$	$-2^{25}5^{17}$	(0,5)	T_{36}	60	$C_{30}C_2$

continued on next page

TABLE A.24: All decics from Tables A.18 and A.19 having class number $h \geq 32$. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^{10} - 15x^8 + 250x^6 - 6250x^4 + 42950x^2 + 15210$	$-2^{27}5^{17}$	(0,5)	T_{36}	60	$C_{30}C_2$
$x^{10} + 80x^8 + 2300x^6 + 32400x^4 + 229500x^2 + 655360$	$-2^{33}5^{17}$	(0,5)	T_{39}	60	$C_{30}C_2$
$x^{10} + 40x^8 + 390x^6 + 520x^4 + 180x^2 + 8$	$-2^{21}5^{18}$	(0,5)	T_{29}	62	C_{62}
$x^{10} - x^9 + 12x^8 - 35x^7 + 291x^6 - 204x^5 + 949x^4 + 1659x^3 + 3767x^2 - 16760x + 42096$	$-17^7 19^7$	(0,5)	T_{22}	64	$C_{16}C_4$
$x^{10} - 20x^8 + 170x^6 - 600x^4 + 865x^2 + 324$	$-2^{16}5^{16}$	(0,5)	T_{11}	75	$C_{15}C_5$
$x^{10} - 20x^7 - 5x^6 + 92x^5 + 200x^4 + 260x^3 + 225x^2 + 120x + 32$	$-2^{18}5^{16}$	(0,5)	T_{11}	75	$C_{15}C_5$
$x^{10} - x^9 + 45x^8 - 45x^7 + 749x^6 - 749x^5 + 5677x^4 - 5677x^3 + 19757x^2 - 19757x + 31021$	$-11^9 17^5$	(0,5)	T_1	82	C_{82}
$x^{10} + 40x^8 + 400x^6 + 1000x^4 + 800x^2 + 160$	$-2^{15}5^{17}$	(0,5)	T_1	82	C_{82}
$x^{10} + 39x^8 + 390x^6 + 1274x^4 + 923x^2 + 117$	$-2^{30}13^9$	(0,5)	T_{29}	84	$C_{42}C_2$
$x^{10} + 10x^8 + 50x^6 + 100x^4 + 100x^2 + 40$	$-2^{25}5^{17}$	(0,5)	T_{36}	90	$C_{30}C_3$
$x^{10} - 50x^6 + 200x^4 - 250x^2 + 100$	$-2^{24}5^{16}$	(0,5)	T_{36}	96	C_{96}
$x^{10} + 58x^8 + 928x^6 + 3712x^4 + 59392$	$-2^{25}29^9$	(0,5)	T_{39}	108	$C_{54}C_2$
$x^{10} + 25x^6 + 500x^4 + 275x^2 + 10$	$-2^{23}5^{19}$	(0,5)	T_{39}	108	$C_{54}C_2$
$x^{10} + 50x^8 + 875x^6 + 6250x^4 + 15625x^2 + 250$	$-2^{19}5^{19}$	(0,5)	T_5	112	$C_{56}C_2$
$x^{10} + 50x^8 + 2300x^6 + 57000x^4 + 523300x^2 + 1011240$	$-2^{29}5^{19}$	(0,5)	T_{39}	112	$C_{56}C_2$
$x^{10} + 25x^8 + 200x^6 + 1000x^4 + 2500x^2 + 4500$	$-2^{20}5^{17}$	(0,5)	T_{23}	120	$C_{60}C_2$
$x^{10} + 25x^8 + 200x^6 + 650x^4 + 800x^2 + 180$	$-2^{18}5^{19}$	(0,5)	T_{29}	120	C_{120}
$x^{10} - 10x^8 + 1600x^2 + 5760$	$-2^{23}5^{17}$	(0,5)	T_{36}	120	$C_{60}C_2$
$x^{10} - 10x^8 - 10x^7 - 200x^6 + 412x^5 + 1150x^4 - 685x^3 + 11690x^2 - 38700x + 33976$	$-3^{13}5^{17}$	(0,5)	T_{11}	130	C_{130}
$x^{10} + 40x^8 + 620x^6 + 4640x^4 + 16700x^2 + 23040$	$-2^{33}5^{13}$	(0,5)	T_{29}	144	$C_{36}C_2C_2$
$x^{10} + 20x^8 + 140x^6 + 400x^4 + 380x^2 + 16$	$-2^{30}5^{12}$	(0,5)	T_{29}	150	C_{150}
$x^{10} + 20x^8 + 200x^6 + 1040x^4 + 3420x^2 + 10368$	$-2^{23}5^{16}$	(0,5)	T_{36}	150	$C_{30}C_5$
$x^{10} + 10x^8 + 125x^6 + 250x^4 + 175x^2 + 40$	$-2^{23}5^{17}$	(0,5)	T_{36}	180	$C_{30}C_6$
$x^{10} + 24x^8 + 194x^6 + 588x^4 + 431x^2 + 4$	$-2^{30}13^8$	(0,5)	T_{29}	222	C_{222}
$x^{10} + 10x^8 + 25x^6 - 50x^4 - 25x^2 + 40$	$-2^{23}5^{17}$	(0,5)	T_{36}	240	$C_{120}C_2$
$x^{10} + 52x^8 + 702x^6 + 2236x^4 + 2223x^2 + 416$	$-2^{33}13^9$	(0,5)	T_{29}	392	$C_{98}C_2C_2$
$x^{10} + 50x^8 + 550x^6 + 2300x^4 + 3500x^2 + 640$	$-2^{21}5^{19}$	(0,5)	T_{29}	404	$C_{202}C_2$
$x^{10} - x^9 + 78x^8 - 78x^7 + 2234x^6 - 2234x^5 + 28645x^4 - 28645x^3 + 160700x^2 - 160700x + 345577$	$-11^9 29^5$	(0,5)	T_1	550	C_{550}

Table A.25: All decics from Tables A.21 and A.22.

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^{10} - 2x^9 + 3x^8 - 3x^6 + 6x^5 - 3x^4 - 24x^3 + 3x^2 + 22x + 13$	$-2^{22}3^9$	(0,5)	T_5	1	C_1
$x^{10} - 4x^9 + 6x^8 - 8x^7 + 11x^6 - 12x^5 + 26x^4 - 32x^3 + 27x^2 - 16x + 4$	$-2^{16}3^{13}$	(0,5)	T_{40}	1	C_1
$x^{10} - 4x^9 + 2x^8 + 12x^7 - 13x^6 - 8x^5 + 12x^4 + 4x^3 - x^2 - 8x + 4$	$-2^{18}3^{12}$	(0,5)	T_{43}	1	C_1
$x^{10} - 4x^9 + 8x^8 - 12x^7 + 17x^6 - 20x^5 + 30x^4 - 44x^3 + 41x^2 - 20x + 4$	$-2^{18}3^{13}$	(0,5)	T_{22}	1	C_1
$x^{10} - 2x^9 - 8x^7 + 22x^6 - 12x^5 + 48x^4 - 96x^3 + 36x^2 - 72x + 144$	$-2^{22}3^{11}$	(0,5)	T_{22}	1	C_1
$x^{10} - x^9 + 9x^8 + 30x^6 + 18x^5 + 54x^4 + 48x^3 + 45x^2 + 35x + 13$	$-2^{18}3^{14}$	(0,5)	T_{43}	1	C_1
$x^{10} - 3x^9 - x^8 + 20x^7 - 20x^6 - 44x^5 + 64x^4 + 32x^3 - 73x^2 + 15x + 61$	$-2^{20}3^{13}$	(0,5)	T_{41}	1	C_1
$x^{10} - 2x^9 + 2x^8 - 12x^7 + 17x^6 - 10x^5 + 30x^4 - 28x^3 + 17x^2 - 10x + 4$	$-2^{20}3^{13}$	(0,5)	T_{22}	1	C_1
$x^{10} - x^9 - 3x^8 + 18x^7 - 3x^6 - 75x^5 + 27x^4 + 114x^3 - 39x^2 - 55x + 25$	$-2^{22}3^{12}$	(0,5)	T_{43}	1	C_1
$x^{10} + 2x^8 - 8x^7 + 13x^6 - 4x^5 - 2x^4 - 20x^3 + 65x^2 - 36x + 16$	$-2^{22}3^{13}$	(0,5)	T_{22}	1	C_1
$x^{10} - x^9 - 3x^8 + 20x^7 - 8x^6 - 36x^5 + 84x^4 - 48x^3 - 144x + 144$	$-2^{22}3^{13}$	(0,5)	T_{22}	1	C_1
$x^{10} - 2x^9 + 24x^7 - 18x^6 - 108x^5 - 24x^4 + 144x^3 + 180x^2 + 88x + 16$	$-2^{22}3^{13}$	(0,5)	T_{41}	1	C_1
$x^{10} - 4x^9 + 12x^8 - 24x^7 + 46x^6 - 72x^5 + 88x^4 - 72x^3 + 45x^2 - 20x + 4$	$-2^{29}3^6$	(0,5)	T_{43}	1	C_1
$x^{10} - 2x^9 + 2x^8 - 8x^7 + 6x^6 + 4x^5 + 12x^4 - 8x^3 + x^2 - 2x + 2$	$-2^{26}3^8$	(0,5)	T_5	1	C_1
$x^{10} + 5x^8 + 4x^6 - 36x^2 + 36$	$-2^{20}3^{12}$	(0,5)	T_{22}	1	C_1
$x^{10} + 10x^6 + 28x^4 + 9x^2 + 4$	$-2^{24}3^{10}$	(0,5)	T_{22}	1	C_1
$x^{10} - 4x^8 - 8x^7 + 4x^6 + 32x^5 + 32x^4 - 32x^3 - 56x^2 + 32$	$-2^{24}3^{10}$	(0,5)	T_{41}	1	C_1
$x^{10} + 4x^8 - 14x^6 - 20x^4 + 49x^2 + 16$	$-2^{26}3^{10}$	(0,5)	T_{22}	1	C_1
$x^{10} - 7x^8 - 8x^7 + 16x^6 + 32x^5 + 16x^4 - 8x^3 - 7x^2 + 1$	$-2^{26}3^{10}$	(0,5)	T_{22}	1	C_1
$x^{10} - 4x^9 + 12x^8 - 16x^7 + 4x^6 + 48x^5 - 96x^4 + 96x^3 + 72x^2 - 288x + 288$	$-2^{28}3^{10}$	(0,5)	T_{41}	1	C_1
$x^{10} - 2x^9 - 3x^8 + 16x^7 - 8x^6 - 24x^5 + 52x^4 - 8x^3 + 9x^2 - 2x + 1$	$-2^{29}3^{10}$	(0,5)	T_{43}	1	C_1
$x^{10} - 4x^9 - 4x^8 + 24x^7 + 6x^6 - 56x^5 + 40x^4 + 8x^3 - 11x^2 - 4x + 4$	$-2^{29}3^{10}$	(0,5)	T_{43}	1	C_1
$x^{10} - 2x^9 - 7x^8 + 32x^7 - 20x^6 - 72x^5 + 196x^4 - 224x^3 + 149x^2 - 58x + 13$	$-2^{26}3^{12}$	(0,5)	T_{22}	1	C_1
$x^{10} - 4x^8 - 8x^7 + 28x^6 + 32x^5 - 64x^4 - 80x^3 + 244x^2 - 192x + 80$	$-2^{27}3^{12}$	(0,5)	T_{43}	1	C_1
$x^{10} - 4x^9 + 8x^8 - 24x^7 + 62x^6 - 56x^5 + 40x^4 - 72x^3 - 83x^2 + 188x + 200$	$-2^{29}3^{12}$	(0,5)	T_{43}	1	C_1
$x^{10} - 2x^9 - 19x^8 + 56x^7 + 70x^6 - 444x^5 + 622x^4 - 368x^3 + 122x^2 - 52x + 34$	$-2^{29}3^{12}$	(0,5)	T_{43}	1	C_1
$x^{10} + 2x^8 + 10x^6 - 8x^4 - 7x^2 - 2$	$2^{25}3^8$	(2,4)	T_4	1	C_1
$x^{10} + 2x^8 - 8x^7 - 8x^6 - 16x^5 - 16x^4 - 8x^3 - 14x^2 - 4$	$2^{27}3^8$	(2,4)	T_{40}	1	C_1

continued on next page

TABLE A.25: All decics from Tables A.21 and A.22. (*cont.*)

Defining Polynomial	d_L	(r,s)	G	h	$\mathcal{C}_L$
$x^{10} - 2x^9 - x^8 + 8x^7 + x^6 - 6x^5 - 11x^4 + 4x^3 + 14x^2 - 4x - 2$	$-2^{21}3^{12}$	(4,3)	T_{43}	1	C_1
$x^{10} - 6x^8 - 8x^7 + 19x^6 + 36x^5 - 46x^4 - 20x^3 + 15x^2 + 12x - 4$	$2^{25}3^{10}$	(6,2)	T_{22}	1	C_1
$x^{10} - 2x^9 + 5x^8 - 8x^7 + 3x^6 - 14x^5 - 3x^4 - 8x^3 - 5x^2 - 2x - 1$	$2^{25}3^{10}$	(2,4)	T_{22}	1	C_1
$x^{10} - 2x^9 - x^8 + 12x^7 - 6x^6 + 4x^5 + 10x^4 - 8x^3 + 10x^2 - 4x + 2$	$2^{25}3^{10}$	(2,4)	T_{22}	1	C_1
$x^{10} - 2x^9 - x^8 - 10x^6 - 4x^5 - 2x^4 + 10x^2 + 4x + 2$	$-2^{28}3^{10}$	(4,3)	T_{43}	1	C_1
$x^{10} - 4x^9 + 8x^8 - 16x^7 + 12x^6 - 16x^5 + 32x^3 - 8x^2 + 32x + 32$	$-2^{28}3^{10}$	(4,3)	T_{43}	1	C_1
$x^{10} - 6x^6 - 8x^4 - 39x^2 - 72$	$2^{25}3^{12}$	(2,4)	T_{12}	1	C_1
$x^{10} - 2x^9 - 3x^8 - 8x^7 + 4x^6 - 48x^5 + 4x^4 - 8x^3 - 3x^2 - 2x + 1$	$2^{27}3^{12}$	(2,4)	T_{12}	1	C_1
$x^{10} - 4x^8 - 8x^7 + 34x^6 - 40x^5 - 4x^4 + 88x^3 - 95x^2 + 24x + 8$	$2^{27}3^{12}$	(2,4)	T_{40}	1	C_1
$x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$	-11^9	(0,5)	T_1	1	C_1
$x^{10} - x^9 + 5x^8 - 2x^7 + 16x^6 - 7x^5 + 20x^4 + x^3 + 12x^2 - 3x + 1$	$-3^5 11^8$	(0,5)	T_1	1	C_1
$x^{10} - x^9 - 10x^8 + 10x^7 + 34x^6 - 34x^5 - 43x^4 + 43x^3 + 12x^2 - 12x + 1$	$3^5 11^9$	(10,0)	T_1	1	C_1
$x^{10} - 3x^9 + 7x^8 - 12x^7 + 15x^6 - 15x^5 + 12x^4 - 7x^3 + 4x^2 - 2x + 1$	$-7^5 11^4$	(0,5)	T_6	1	C_1
$x^{10} - 3x^9 + x^8 + 8x^7 - 17x^6 + 15x^5 + 16x^4 - 68x^3 + 84x^2 - 49x + 16$	$-7^7 11^6$	(0,5)	T_{22}	1	C_1
$x^{10} - 5x^9 + 13x^8 - 22x^7 + 27x^6 - 25x^5 + 16x^4 - 6x^3 + 5x^2 - 4x + 1$	$-7^6 11^7$	(0,5)	T_{22}	1	C_1
$x^{10} - x^9 - 17x^8 + 9x^7 + 126x^6 + 48x^5 - 486x^4 - 648x^3 + 738x^2 + 1350x + 837$	$-3^{13}11^8$	(0,5)	T_{11}	5	C_5
$x^{10} - 5x^9 + 7x^8 + 2x^7 - 16x^6 + 20x^5 - 8x^4 - 5x^3 + 16x^2 - 12x + 21$	$-3^{13}11^8$	(0,5)	T_{11}	5	C_5
$x^{10} - 5x^9 + 25x^8 - 70x^7 + 152x^6 - 232x^5 + 423x^4 - 531x^3 + 741x^2 - 504x + 441$	$-3^{12}11^9$	(0,5)	T_{11}	5	C_5
$x^{10} - 4x^9 + 16x^8 - 9x^7 + 3x^6 + 186x^5 - 73x^4 + 358x^3 + 581x^2 - 168x + 1068$	$-3^{12}11^9$	(0,5)	T_{11}	5	C_5
$x^{10} - 3x^9 - 2x^8 + 50x^7 - 128x^6 - 100x^5 + 1048x^4 - 1153x^3 - 1898x^2 + 3879x - 857$	$3^{13}11^9$	(2,4)	T_{11}	5	C_5
$x^{10} - 5x^9 - 8x^8 + 62x^7 + 20x^6 - 298x^5 - 50x^4 + 679x^3 + 235x^2 - 636x - 384$	$3^{13}11^9$	(2,4)	T_{11}	5	C_5
$x^{10} - 3x^8 + 19x^6 - 11x^5 - 40x^4 + 55x^3 + 23x^2 - 44x + 32$	$-7^5 11^8$	(0,5)	T_6	5	C_5
$x^{10} - 3x^8 + 19x^6 + 37x^4 - 54x^2 + 175$	$-7^5 11^8$	(0,5)	T_2	5	C_5
$x^{10} - x^9 + 14x^8 - 7x^7 + 85x^6 - 29x^5 + 218x^4 - 8x^3 + 216x^2 - 48x + 32$	$-7^5 11^8$	(0,5)	T_1	5	C_5
$x^{10} - 2x^9 + 4x^8 - 8x^7 + 5x^6 + 12x^5 + 31x^4 + 48x^3 + 80x^2 + 27x + 45$	$-7^4 11^9$	(0,5)	T_3	5	C_5