Tetrakaidecic Extensions of $\mathbb{Q}_p$

Robert Cass, Salvatore Parenti, Daniel Shankman

July 10, 2013

Contents

1 Introduction

For a prime p and a positive integer n, it is well-known that there are only finitely many degree n field extensions of the field $\mathbb{Q}_p$ of p-adic numbers. When p does not divide n or $p = n$, the extensions of $\mathbb{Q}_p$ have been classified and data associated to these extensions is stored in an online database of local fields created by John W. Jones and David P. Roberts. When p properly divides n, the problem of classifying these extensions becomes more complicated. In this case, such extensions have been classified completely for $n \leq 12$.

In our work, we focus on the case $n = 14$ and $p = 2$ or $p = 7$. We use methods established by Sebastian Pauli and Xavier-François Roblot to find defining polynomials for each of these extensions up to isomorphism. Employing computational methods similar to those used by Chad Awtrey to classify degree 12 extensions of $\mathbb{Q}_3$, we compute several invariants associated to these extensions to determine the Galois groups of their defining polynomials. The primary invariants we use for determining the Galois groups are the subfield content, the size of the automorphism group, and the parity. In the cases in which these invariants are insufficient to distinguish the Galois groups, we use resolvent polynomials. Additionally, we present a conjecture about the number of totally ramified extensions of $\mathbb{Q}_p$ for a fixed discriminant and certain choices of p and n.

2 Basic Facts and Notions Regarding $\mathbb{Q}_p$

Here we will state, but not prove, several definitions and results about the field of p-adic numbers, $\mathbb{Q}_p$. For a more detailed treatment of the following material, see [4].

Let p be a prime number. The p-order function $\mathrm{ord}_p : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}$ gives the largest t for which p^t divides a given integer. For example, $\mathrm{ord}_2(32) = 5$, $\mathrm{ord}_7(98) = 2$, and $\mathrm{ord}_{11}(20) = 0$. By convention $\mathrm{ord}_p(0) = \infty$. We have the following two properties of ord_p for integers a, b:

(i) $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$

(ii) $\mathrm{ord}_p(a + b) \geq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$.

A nonzero rational number a may be factored uniquely into a unit and a product of prime factors, i.e. $a = u p_1^{e_1} \cdots p_r^{e_r}$, where $u = \pm 1$, the numbers $p_1, \ldots, p_r$ are primes, and $e_1, \ldots, e_r$ are integers. Thus the domain of ord_p may be extended to $\mathbb{Q} \setminus \{0\}$ by defining $\mathrm{ord}_p(a)$ to be the exponent e. For example, $\mathrm{ord}_7(3/49) = -2$, and $\mathrm{ord}_{13}(39/11) = 1$. Again it is easy to see that properties (i), (ii) above hold for rational numbers a, b.

The p-adic absolute value $|\cdot|_p : \mathbb{Q} \to \mathbb{Q}$ can then be defined by the formula $|a|_p = p^{-\mathrm{ord}_p(a)}$ when a is nonzero, 0 otherwise. This absolute value, which hereafter we designate by $|\cdot|$, is an example of a non-Archimedean absolute value.

A *non-Archimedean* absolute value on a field K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ that satisfies the following three properties for any $a, b, c \in K$:

(i) $|a| \geq 0$ and $= 0$ if and only if $a = 0$

(ii) $|ab| = |a||b|$

(iii) $|a + b| \leq max\{|a|, |b|\}$

We induce a metric from a non-Archimedean absolute value on K, by defining the distance between two points to be the absolute value of their difference. There are many interesting properties that follow from a non-Archimedean absolute value and its induced metric.

Facts ($a, b, c \in K$ and $0 \le r \in \mathbb{R}$:

(i) All triangles are isosceles, i.e. $|a-b|$ is equal to $|a-c|$ or $|b-c|$.

(ii) If $|a| \neq |b|$ then property (iii) above can be replaced by $|a+b| = \max\{|a|, |b|\}$.

(iii) An open (resp. closed) ball centered about a point with a fixed radius will also be a closed (resp. open) set.

(iv) Let $B(a,r)$ denote the open ball with center a and radius r, and let $\bar{B}(a,r)$ be its closure. For either ball, if $b \in B(a,r)$ (resp. $\bar{B}(a,r)$), then $B(a,r) = B(b,r)$ (resp. $\bar{B}(a,r) = \bar{B}(b,r)$). In other words, any point contained in a ball with a fixed center and radius will be the center of that ball with the same radius.

(v) For a sequence to be Cauchy, it is only necessary that the distance between consecutive terms go to zero.

(vi) As long as the terms in an infinite series converge to 0 in absolute value, the series will be Cauchy.

In particular, all of these results hold for $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot| := |\cdot|_p$. Just as the set of real numbers $\mathbb{R}$ is defined to be the completion of $\mathbb{Q}$ with respect to the usual absolute value, the set of *p-adic numbers* $\mathbb{Q}_p$ is defined to be the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. It follows that the p-adic absolute value when extended to $\mathbb{Q}_p$ remains non-Archimedean, so again all of the above facts hold.

Formally, $\mathbb{Q}_p$ is the ring C of Cauchy sequences in $\mathbb{Q}$ (i.e. $\{A \in \prod_{i=0}^{\infty} \mathbb{Q} : \lim_{n\to\infty} |A(n+1) - A(n)| = 0\}$) modded out by the maximal ideal $M = \{A \in C : \lim_{n\to\infty} A(n) = 0\}$. The field $\mathbb{Q}$ may be embedded into $\mathbb{Q}_p$ via the mapping $x \to (x, x, x, ...) + M$. However, we need not be so formal. If we regard $\mathbb{Q}$ as a subset of $\mathbb{Q}_p$, every element of $\mathbb{Q}_p$ may be described in terms of integers as follows:

Theorem 2.1. *Every element of $\mathbb{Q}_p$ can be written as an infinite series $\sum_{i=k}^{\infty} a_i p^i$, with each $a_i \in \{0, 1, ..., p-1\}$ and $k \in \mathbb{Z}$. For every p-adic number, the numbers $a_k, a_{k+1}, ...$ composing its series are uniquely determined.*

Proof. See [4] pg. 68. □

Adding and multiplying elements of $\mathbb{Q}_p$, written in the above form, works exactly like adding and multiplying formal power series in the indeterminate 'p'. The resulting series can then be rewritten in "base p." (insert example).

The p-order function can be extended to $\mathbb{Q}_p$ in the obvious way: for a p-adic number, as $A = \sum_{i=k}^{\infty} a_i p^i = p^k(\sum_{i=0}^{\infty} a_{i+k} p^i)$, the sum $\sum_{i=0}^{\infty} a_{i+k} p^i$ is not divisible by p, so we may define $\mathrm{ord}_p(A)$ to be k in this case. We may then extend the p-adic absolute value to $\mathbb{Q}_p$ by defining $|A|$ to be $p^{-\mathrm{ord}_p(A)}$. The extended absolute value on $\mathbb{Q}_p$ remains non-Archimedean.

In $\mathbb{Q}_p$, we have the associated valuation ring $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a| \le 1\} = \{a \in \mathbb{Q}_p : \mathrm{ord}_p(a) \ge 0\}$, and its unique maximal ideal $p\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a| < 1\} = \{a \in \mathbb{Q}_p : \mathrm{ord}_p(a) > 0\}$. The names are fitting: $\mathbb{Z}_p$, the set of *p-adic integers*, is the completion of $\mathbb{Z}$ in $\mathbb{Q}_p$, and $p\mathbb{Z}_p$ is the ideal generated by the prime number p in $\mathbb{Z}_p$. From Theorem 2.1 it is clear that every p-adic number may be written as an integral power of p multiplied by some p-adic integer. In later sections we will investigate non-field integral domains containing $\mathbb{Z}_p$, so it will be useful when denoting principal ideals to mention the ring in which the ideal is generated, as $p\mathbb{Z}_p$ rather than (p).

The quotient ring $\mathbb{Z}_p/p\mathbb{Z}_p$ is a field, called the *residue field* of $\mathbb{Q}_p$. For a typical element $\sum_{i=0}^{\infty} a_i p^i + p\mathbb{Z}_p$, the terms $a_1 p, a_2 p^2$ etc. being divisible by p will vanish, leaving just

$a_0 \in \{0, 1, ..., p-1\}$. The residue field is thus isomorphic to the integers modulo p, so we will denote it by $\mathbb{F}_p$.

One last thing to mention is Hensel's Lemma, named after the mathematician that introduced p-adic numbers in 1897.

Theorem (Hensel's Lemma) 2.2. *Let $f \in \mathbb{Z}_p[X]$, and let $\bar{f}$ be the corresponding polynomial in $\mathbb{F}_p[X]$. Suppose $\bar{a} = a + p\mathbb{Z}_p \in \mathbb{F}_p$ is such that $\bar{f}(\bar{a}) = 0$ but $\bar{f}'(\bar{a}) \neq 0$. Then there exists some $b \in \mathbb{Z}_p$ such that $b + p\mathbb{Z}_p = a + p\mathbb{Z}_p$ and $f(b) = 0$.*

Proof. [4] pg. 70. □

3 Finite Dimensional Extensions of $\mathbb{Q}_p$

Let L be a finite of a field K of characteristic zero, say $[L : K] = n$. We have a multiplicative map $N_{L/K} : L \to K$, called the *norm* of L over K, which can be defined in three equivalent ways:

(i) For $a \in L$, let $\phi_a : L \to L$ be given by $\phi_a(y) = ay$. As a K-linear transformation, ϕ_a may be represented by a matrix $A \in \mathrm{Mat}_n(K)$. We then define $N_{L/K}(a)$ to be $\det(A)$.

(ii) Let $m_a \in K[X]$ be the minimal polynomial of a over K. Then $N_{L/K}(a) := (-1)^{n \cdot deg(\mu)} m_a(0)^{deg(\mu)}$.

(iii) If $\overline{K}$ is any algebraic closure of K, since $\mathrm{Char}(K) = 0$ there are exactly n K-monomorphisms of L into $\overline{K}$, say $\sigma_1, ..., \sigma_n$. Then $N_{L/K}(a) := \prod_{i=1}^{n} \sigma_i(a)$. Note that if (and only if) L is Galois over K, every K-monomorphism of L into $\overline{K}$ is actually a K-automorphism, so $N_{L/K}(a) = \prod_{\sigma \in \mathrm{Aut}(L/K)} \sigma(a)$, where $\mathrm{Aut}(L/K)$ is the group of K-automorphisms of L.

For our purposes, we need not worry about the field norm for fields of prime characteristic; we only use it for finite dimensional extensions of $\mathbb{Q}_p$. Note that the composition of norms works out nicely, i.e. if $K \subseteq E \subseteq F$ are fields for which the norm is defined, then $N_{F/K} = N_{E/K} \circ N_{F/E}$.

We now assume K is an n-dimensional extension of $\mathbb{Q}_p$, and let $v_1, ..., v_n$ be a basis.

Using the field norm, we may extend the p-adic absolute value to K by defining $|a|$ to be $\sqrt[n]{|N_{K/\mathbb{Q}_p}(a)|}$. This extended absolute value remains non-Archimedean, and K will still be complete with respect to this absolute value.

Intuitively since a sequence in K may be written as $a_{1,i}v_1 + ... + a_{n,i}v_n$ with the limit distributing over addition, there is really one place for a convergent sequence to converge to. Thus any two absolute values on K which restrict to the p-adic absolute value on $\mathbb{Q}_p$ must induce the same topology on K. And since two absolute values $||_1$ and $||_2$ on a field K induce the same topology if and only if there exists a real number δ such that $||_1 = ||_2^{\delta}$ (this is not a trivial result, see F. Gouvea's book), it is clear that there can only be one absolute value on K which restricts to the p-adic absolute value on $\mathbb{Q}_p$.

Since $|a| = p^{-\mathrm{ord}_p(a)}$ for $a \in \mathbb{Q}_p$, we have $\mathrm{ord}_p(a) = -\log_p |a|$, so we can naturally extend the domain ord_p to $K \setminus \{0\}$ by defining $\mathrm{ord}_p(a)$ to be $-\log_p |a|$. Thus we have an order-reversing bijection between the image of the absolute value and the image of the p-order. Moreover, we have $\mathrm{ord}_p(a) = \frac{\mathrm{ord}_p(N_{K/\mathbb{Q}_p}(a))}{n}$. Now the p-order can take on rational values. The following theorem gives a more precise formulation of the image of ord_p.

Theorem 3.1. *There exists a divisor e of n such that $\mathrm{ord}_p(K \setminus \{0\}) = \frac{1}{e}\mathbb{Z}$. In particular, the norm $N_{K/\mathbb{Q}_p}$ is never surjective.*

Proof. ord_p is a group homomorphism from $K\setminus\{0\}$ to $\mathbb{Q}$, so $ord_p(K\setminus\{0\})$ is an additive subgroup of $\mathbb{Q}$. Since for any $0 \neq a \in K$, $\mathrm{ord}_p(a) = \frac{\mathrm{ord}_p(N(a))}{n}$, it follows that $ord_p(K \setminus \{0\}) \subseteq \frac{1}{n}\mathbb{Z}$.

But $\frac{1}{n}\mathbb{Z}$ is a cyclic group generated by $1/n$, and its nontrivial subgroups are also cyclic, taking the form $\frac{1}{d}\mathbb{Z}$ where d is a divisor of n. $\mathrm{ord}_p(K \setminus \{0\})$ being a nontrivial subgroup of $\frac{1}{n}\mathbb{Z}$, the assertion is then obvious. $\square$

As in $\mathbb{Q}_p$, we have the *ring of integers of* K, defined to be $\mathcal{O}_K = \{a \in K : |a| \leq 1\} = \{a \in K : \mathrm{ord}_p(a) \geq 0\}$, and its unique maximal ideal $\mathfrak{M}_K = \{a \in K : |a| < 1\} = \{a \in K : \mathrm{ord}_p(a) > 0\}$. Thus a is a unit in $\mathcal{O}_K$ if and only if $\mathrm{ord}_p(a) = 0$. Just as $\mathbb{Z}_p$ is a complete subspace of $\mathbb{Q}_p$, so is $\mathcal{O}_K$ of K.

The residue field $k := \mathcal{O}_K/\mathfrak{M}_K$ contains an isomorphic copy of $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$. This can be conveyed by the following diagram:

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[r, hook] \arrow[d, "\phi"] \arrow[dr, "\psi_{|\mathbb{Z}_p}"] & \mathcal{O}_K \arrow[d, "\psi"] \\
\mathbb{Z}_p/p\mathbb{Z}_p \arrow[r, phantom, "\delta"] & \mathcal{O}_K/\mathfrak{M}_K
\end{tikzcd}$$

Here ϕ, ψ are the canonical epimorphisms, each of which sends an element to its coset, and δ is the unique monomorphism such that $\delta \circ \phi = \psi_{|\mathbb{Z}_p}$. In place of $\psi(a) = a + \mathfrak{M}_K$ or $\phi(b) = b + \mathbb{Z}_p$ we may write $\bar{a}$ or $\bar{b}$ where appropriate.

There is no trouble in identifying $\mathbb{F}_p$ with its isomorphic copy $\delta(\mathbb{F}_p)$ in k. We will briefly return to the formality of isomorphic inclusions in section four, but in general we will not dwell upon it.

Theorem 3.2. *The residue field k is finite.*

Proof. Since $\mathcal{O}_K$ is totally bounded (as a closed ball of radius 1) and complete, it is a compact subspace of K. Note $\mathfrak{M}_K$ is an open set (as an open ball of radius 1). For every $a \in \mathcal{O}_K$, the function $f_a : \mathcal{O}_K \to \mathcal{O}_K$ given by $f_a(b) = a + b$ is a homeomorphism, making each coset $a + \mathfrak{M}_K$ an open set. Since $\mathcal{O}_K$ is equal to $\bigcup_{a \in \mathcal{O}_K} a + \mathfrak{M}_K$, k must have only finitely many members by compactness. $\square$

Theorem 3.3. *$\mathcal{O}_K$ is a principal ideal domain.*

Proof. Let I be any ideal of $\mathcal{O}_K$. By Theorem 3.1, it is possible to choose some $\pi \in I$ such that $\mathrm{ord}_p(\pi)$ is minimal (i.e. $|\pi|$ is maximal). We claim that $\pi\mathcal{O}_K = I$. If $y \in I$, then $|y| \leq |\pi|$, meaning $y\pi^{-1} \in \mathcal{O}_K$. But then $y = \pi(y\pi^{-1})$, meaning $y \in \pi\mathcal{O}_K$. $\square$

Any generator of the maximal ideal $\mathfrak{M}_K$ is called a *uniformizer* of K (sometimes also called a uniformizer of $\mathcal{O}_K$). We will typically denote a uniformizer by ϖ_K. Since a principal ideal of an element is also generated by that element's associates, and the units of $\mathcal{O}_K$ are precisely those members with absolute value 1, it follows that all generators of an ideal have the same absolute value, i.e. π generates I if and only if $|\pi|$ is maximal among elements of I.

Corollary 3.4. *Every ideal of $\mathcal{O}_K$ is equal to $\varpi_K^d\mathcal{O}_K$ for some $d \in \mathbb{N}$.*

Proof. Let I be an ideal of $\mathcal{O}_K$ generated by π. Since $\mathcal{O}_K$ is a local principal ideal domain, the element ϖ_K is up to associates the only irreducible element of $\mathcal{O}_K$. Moreover every PID is a unique factorization domain, so we can write π as $\varpi_K^d b$ for some $d \in \mathbb{N}$ and unit b. But this just means that $I = \pi\mathcal{O}_K = \varpi_K^d \mathcal{O}_K$. $\square$

By the previous corollary since $p \in \mathcal{O}_K$, there exists a number $e_K \in \mathbb{N}$ such that the ideal generated by p is equal to the ideal generated by $\varpi_K^{e_K}$. e_K is called the *ramification index* of K over $\mathbb{Q}_p$. The ramification index is unique because $\varpi, \varpi^2, \varpi^3, ...$ all have different absolute values, and elements with different absolute values generate distinct principal ideals.

Lemma 3.5. *The following conditions are equivalent for a natural number $e \in \mathbb{N}$:*

(i) e is the ramification index of K over $\mathbb{Q}_p$.

(ii) Let ϖ_K generate $\mathfrak{M}_K$. Then ϖ_K^e and p are associates in $\mathcal{O}_K$.

(iii) $\mathrm{ord}_p(K \setminus \{0\}) = \frac{1}{e}\mathbb{Z}$

Proof. Clearly (i) and (ii) are equivalent. For (iii) implies (ii) (from which (i) implies (iii) follows by uniqueness of the ramification index), note that ϖ_K was chosen to have maximal absolute value strictly less than 1, i.e. minimal p-order strictly greater than 0. Thus $\mathrm{ord}_p(\varpi_K) = 1/e$, since $1/e$ is the smallest positive number in the image of $\mathrm{ord}_p(K \setminus 0)$. Then $\mathrm{ord}_p(\varpi_K^e) = e \cdot \mathrm{ord}_p(\varpi_K) = 1 = \mathrm{ord}_p(p)$, so $|\varpi_K^e| = |p|$, making ϖ_K^e and p associates in $\mathcal{O}_K$. $\square$

Thus by Lemma 3.5 and Theorem 3.1, e_K must be a divisor of n. When $e_K = 1$, K is called an *unramified* extension of $\mathbb{Q}_p$, and when $e_K = n$, K is said to be *totally ramified.* When e_K is divisible by p, K is called a *wildly ramified* extension of $\mathbb{Q}_p$ and if $p \nmid e_K$, *tamely ramified.*

The index of the residue field k over $\mathbb{F}_p$ is denoted f_K, or just f.

Theorem 3.6. $[K : \mathbb{Q}_p] = e_K f_K$

Proof. $\square$

Just as the p-adic numbers have a unique representation as an infinite series, so do the elements of K.

Theorem 3.7. *If $0, c_1, ..., c_{p^f-1} \in \mathcal{O}_K$ are a complete set of coset representatives for k, then every $a \in K$ is equal to an infinite series $\sum_{i=k}^{\infty} a_i \varpi_K^i$, with each $a_i \in \{0, c_1, ..., c_{p^f-1}\}$. Furthermore a is uniquely determined by the elements a_0, a_1 etc.*

Proof. (do later) $\square$

Let $\phi \in \mathrm{Aut}(K/\mathbb{Q}_p)$. Since $|\cdot| \circ \phi$ is also an absolute value on K which restricts to the p-adic absolute value on $\mathbb{Q}_p$, the uniqueness of such an absolute value gives us $|\phi(a)| = |a|$ for all $a \in K$. In particular, since the Galois group of a splitting field of an irreducible polynomial acts transitively on its roots, all the roots of an irreducible polynomial have the same absolute value and p-order. This is a very useful fact which we will mention many times in the proceeding discussion.

Lemma 3.8. *If $f \in \mathbb{Z}_p[X]$ is monic with $f = gh$ for some monic polynomials $g, h \in \mathbb{Q}_p[X]$, then $g, h \in \mathbb{Z}_p[X]$.*

Proof. Every element of $\mathbb{Q}_p$ can be written as $p^m u$ for some $m \in \mathbb{Z}$ and $u \in \mathbb{Z}_p$, so let $a, b \in \mathbb{Z}$ be such that $g_0 := p^a g$ and $h_0 := p^b h$ are in $\mathbb{Z}_p[X]$ with some coefficient in both g_0 and h_0 having p-order zero.

For this to happen, we cannot have $a < 0$ or $b < 0$. If, say, $a < 0$, then $|p^a| > 1$, meaning the leading coefficient of $g_0 = p^a g$ has absolute value strictly greater than one, since g is monic. This contradicts the assumption that $g_0 \in \mathbb{Z}_p[X]$. Thus a, b and hence $a + b$ are greater than or equal to 0.

But we also cannot have $a + b > 0$. In this case all the coefficients of $p^{a+b} f$ are divisible by p, so the corresponding polynomial $\overline{p^{a+b} f}$ is zero in $\mathbb{F}_p$. On the other hand since at least one of the coefficients of g_0, h_0 has p-order zero, $\overline{g_0}$ and $\overline{h_0}$ and hence $\overline{g_0}\overline{h_0} = \overline{g_0 h_0}$ are nonzero in $\mathbb{F}_p[X]$.

Thus $a + b = 0$, and it follows that $0 = a = b$. Then $g_0 = g$ and $h_0 = h$, i.e. $g, h \in \mathbb{Z}_p[X]$. □

For rings $R \subseteq S$, an element $b \in S$ is *integral* over R if it is the root of a monic polynomial in $R[X]$. The *integral closure* R' of R in S is the set of elements of S which are integral over R. R is called *integrally closed* in S if it is its own integral closure, i.e. if $b \in S$ is the root of a monic polynomial in $R[X]$, then $b \in R$.

Theorem 3.9. *$\mathcal{O}_K$ is the integral closure of $\mathbb{Z}_p$ in K.*

Proof. First, every element in $\mathcal{O}_K$ is integral over $\mathbb{Z}_p$. For suppose $a \in \mathcal{O}_K$ with minimal (monic) polynomial $m_a \in \mathbb{Q}_p[X]$. Let K' be a normal closure of K over $\mathbb{Q}_p$, so that m_a splits completely in $K'[X]$ with roots $a, a', a'', \ldots.$ Since a has absolute value no greater than 1, so do all the rest of the roots $a', a'', \ldots$ Now the coefficients of m_a are additive and multiplicative combinations of the roots of m_a, so they all have absolute value ≤ 1 as well. But these coefficients are in $\mathbb{Q}_p$, so they must be in $\mathbb{Z}_p$.

Conversely suppose $a \in K$ is the root of a monic polynomial $f \in \mathbb{Z}_p$. It is required to show that $a \in \mathcal{O}_K$. Let $m_a \in \mathbb{Q}_p[X]$ be the minimal polynomial of a over $\mathbb{Q}_p$. m_a divides f, so by Lemma 3.8 we have $m_a \in \mathbb{Z}_p[X]$. Now the constant coefficient of m_a is ± 1 times the product of the roots of m_a. This latter coefficient having absolute value less than or equal to 1, there must be a root of m_a with absolute value less than or equal to 1. But all the roots of μ have the same absolute value, so $|a| \leq 1$, i.e. $a \in \mathcal{O}_K$.

□

Hensel's Lemma, stated in section two, can be given in much greater generality. We give a generalization which will be sufficient for our treatment of p-adic extensions in the sequel. [4] gives a nice proof of the original lemma, and the version stated below can be proved in exactly the same way.

Theorem 3.10 (Hensel's Lemma) 1. *If $f \in K[X]$, $a \in K$ with $\bar{f}(a + \mathfrak{M}_K) = 0$ and $\bar{f}'(a + \mathfrak{M}_K) \neq 0$, then there exists some $b \in K$ with $a + \mathfrak{M}_K = b + \mathfrak{M}_K$ and $f(b) = 0$.*

4 Intermediate Fields in the Preceding Discussion

We can extend the p-order on $\mathbb{Q}_p$ to any finite dimensional extension K of $\mathbb{Q}_p$ by defining $\mathrm{ord}_p(a)$ for $a \in K$ to be $\frac{\mathrm{ord}_p(N_{K/\mathbb{Q}_p}(a))}{n}$, where $n = [K : \mathbb{Q}_p]$. However, it is often useful to modify this extended p-order in such a way as to produce a new discrete valuation function taking on integer values. In particular, the discussion of ramification groups in section 9 would be more complicated without this rescaling Here we will investigate the rescaling of the p-order function in a fairly general setting. We let $L_0 = \mathbb{Q}_p \subseteq L_1 \subseteq \cdots L_s$ be a finite chain of finite dimensional field extensions of $\mathbb{Q}_p$. We suppose n_i is the dimension $[L_i : L_{i-1}]$. Thus L_s is $n_1 \cdots n_s$-dimensional over $\mathbb{Q}_p$.

We already know how to extend the p-order function from L_0 to any L_t for $1 \leq t \leq s$. The extension can be done directly, as above, or one field at a time. For example, given that we have already extended the function ord_p to the field L_1, we might emulate the definition above and extend ord_p from L_1 to L_2 by the defining $\mathrm{ord}_p(a)$ for $a \in L_2$ to be $\frac{\mathrm{ord}_p(N_{L_2/L_1}(a))}{n_2}$. But this is the same as defining the extension from $\mathbb{Q}_p$ to L_2 directly, since $\mathrm{ord}_p(a) = \frac{\mathrm{ord}_p(N_{L_2/L_0})(a)}{n_1 n_2} = \frac{1}{n_2} \frac{\mathrm{ord}_p(N_{L_1/L_0} \circ N_{L_2/L_1}(a))}{n_1} = \frac{\mathrm{ord}_p(N_{L_2/L_1}(a))}{n_2}$.

For each field L_i, we have the local principal ideal domain $\mathcal{O}_{L_i}$ and its unique maximal ideal $\mathfrak{M}_{L_i}$. As we have seen, each maximal ideal $\mathfrak{M}_{L_i}$ will be generated by an element ϖ_{L_i} in $\mathcal{O}_{L_i}$ whose p-order is nonzero and minimal. Moreover there must exist a natural number e_{L_i} such that $\varpi_{L_i}^{e_{L_i}}$ is an associate of (that is, has the same p-order as) the element $p \in \mathbb{Z}_p$. Thus $\mathrm{ord}_p(\varpi_{L_i}) = \frac{1}{e_{L_i}}$.

This is all done with respect to the base field $L_0 = \mathbb{Q}_p$. If we begin with a different base field L_t, with maximal ideal $\mathfrak{M}_{L_t} = (\varpi_{L_t})$, and an extension field L_v with $v > t$, then since $\mathcal{O}_{L_v}$ is a PID, there exists some exponent e such that $(\varpi_{L_v}^e) = (\varpi_{L_t})$. This extends the definition of the ramification index to different base fields, from which we can in the obvious fashion define totally ramified, unramified, and tamely ramified extensions in greater generality. Since the ramification index is evidently dependent on both the base field and the extension field, we will denote the aforementioned e by e_{L_v/L_k}. When the base field is $L_0 = \mathbb{Q}_p$, we will not mention the base field and only the extension field, as we have done thus far. Notice in this case that $\mathrm{ord}_p(\varpi_{L_v}^{e_{L_v/L_k}}) = \mathrm{ord}_p(\varpi_{L_t})$, or $\frac{e_{L_v}}{e_{L_k}} = e_{L_v/L_k}$.

The relationship of the various residue fields can be expressed in the following commutative diagram:

$$
\begin{tikzcd}
\mathbb{Z}_p \arrow[r] \arrow[d, "\psi^0"] \arrow[dr, "\psi^1_{|\mathbb{Z}_p}"] & \mathcal{O}_{L_1} \arrow[r] \arrow[d, "\psi^1"] \arrow[dr, "\psi^2_{|\mathcal{O}_{L_1}}"] & \mathcal{O}_{L_2} \arrow[r] \arrow[d, "\psi^2"] \arrow[dr, "\psi^3_{|\mathcal{O}_{L_2}}"] & \mathcal{O}_{L_3} \arrow[r] & \cdots \arrow[r] & \mathcal{O}_{L_s} \\
\mathbb{Z}_p/p\mathbb{Z}_p \arrow[r, "\delta_0"] & \mathcal{O}_{L_1}/\mathfrak{M}_{L_1} \arrow[r, "\delta_1"] & \mathcal{O}_{L_2}/\mathfrak{M}_{L_2} \arrow[r, "\delta_2"] & \mathcal{O}_{L_3}/\mathfrak{M}_{L_3} & \cdots \arrow[r, "\delta_{s-1}"] & \mathcal{O}_{\int}/\mathfrak{M}_{\mathfrak{s}}
\end{tikzcd}
$$

Here ψ^i is the canonical epimorphism, and δ_i is the unique monomorphism satisfying $\delta_i \circ \psi^i \psi^{i+1}_{|\mathfrak{M}_{L_i}}$.

Now each $k_i = \mathcal{O}_{L_i}/\mathfrak{M}_{L_i}$ is a field, and we already know the relationship $[L_i : \mathbb{Q}_p] = e_{L_i}[k_i : \mathbb{F}_p]$. But from the fact that the ramification index is multiplicative we can generalize this fact, since $e_{L_i/L_{i-1}}[k_i : k_{i-1}] = \frac{e_{L_i}}{e_{L_{i-1}}} \frac{[k_i:\mathbb{F}_p]}{[k_{i-1}:\mathbb{F}_p]} = \frac{[L_i:\mathbb{Q}_p]}{[L_{i-1}:\mathbb{Q}_p]} = [L_i : L_{i-1}] = n_i$. Now from this latter relationship, it is easy to see that δ_i is an isomorphism if and only if $[k_{i+1} : k_i] = 1$ if and only if $e_{L_{i+1}/L_i} = n_{i+1}$. Thus, δ_i is an isomorphism if and only if L_{i+1} is a totally ramified extension of L_i.

The latter embedding δ_i is the "standard" way of embedding one residue field in the next. If however, we would like to skip over a few residue fields, for example to embed k_t in k_{t+w}, we may prefer a similar construction, as below:

$$\begin{tikzcd}
\mathcal{O}_t \arrow[r] \arrow[d, "\psi^t"'] \arrow[dr, "\psi^{t+w}_{|\mathcal{O}_t}"] & \mathcal{O}_{t+w} \arrow[d, "\psi^{t+w}"] \\
\mathcal{O}_t/\mathfrak{M}_t \arrow[r, "\Delta"] & \mathcal{O}_{t+w}/\mathfrak{M}_{t+w}
\end{tikzcd}$$

Here Δ is the unique monomorphism satisfying $\Delta \circ \psi^t = \psi^{t+w}_{|M_t}$. As above, we can argue that Δ is an isomorphism if and only if L_{t+w} is a totally ramified extension of L_t. But the map $\psi^{t+w}_{|M_t}$ can be found in the first diagram above, so by uniqueness we have $\Delta = \delta_{t+w-1} \circ \cdots \circ \delta_{t+1} \circ \delta_t$. Since Δ is an isomorphism if and only if each δ_i is an isomorphism, we have:

Theorem 1. *k_{t+w} is a totally ramified extension of k_t if and only if k_{i+1} is a totally ramified extension of k_i for $t \leq i < t+w$.*

Now for $s \geq t \geq 1$, we define the "L_t-order" $\nu_{L_t} : L_t \to \mathbb{Q}$ by $\nu_{L_t} = e_{L_t} \operatorname{ord}_p$. It is easy to see this gives a new valuation on L_t. Since $\operatorname{ord}_p(L_t) = \frac{1}{e_{L_t}}\mathbb{Z}$, $\nu_{L_t}(L_t)$ will take on integer values for $a \in L_t$. In particular where $(\varpi_{L_t}) = \mathfrak{M}_{L_t}$, $\nu_{L_t}(\varpi_{L_t}) = e_{L_t} \operatorname{ord}_p(\varpi_{L_t}) = e_{L_t} \frac{1}{e_{L_t}} = 1$.

Let $t \leq v \leq s$. As with ord_p, we can extend the domain of ν_{L_t} to L_v by defining $\nu_{L_t}(a) = \frac{\nu_{L_t} N_{L_v/L_t}(a)}{[L_v:L_t]} = \frac{\nu_{L_t} N_{L_v/L_t}(a)}{n_v \cdots n_{t+1}}$.

We can of course rescale ν_{L_t} to a new valuation ν_{L_v} in the same way we rescaled ord_p to ν_{L_t}. But the question remains as to whether such a rescaling from ν_{L_t} to ν_{L_v} (that is, by defining ν_{L_v} to be $e_{L_v/L_t}\nu_{L_t}$) would give the same valuation as a rescaling such as we have done above from ord_p to ν_{L_v}. In fact, this is true by the multiplicativity of the ramification index, since $e_{L_v/L_t}\nu_{L_t} = e_{L_v/L_t} e_{L_t} \operatorname{ord}_p = e_{L_v} \operatorname{ord}_p$.

In general for an extension L_t, when $0 \leq w \leq t$ everything we have defined up to this point in the context of local fields-the ring $\mathcal{O}_{L_w}$, the ideal $\mathfrak{M}_{L_w}$, the uniformizer ϖ_{L_w}, the ramification index-can be alternatively and equivalently defined in terms ν_{L_t} instead of ord_p.

The ring $\mathcal{O}_{L_w}$ (resp. the maximal ideal $\mathfrak{M}_{L_w}$) can be defined as the set of members of L_w with nonnegative p-order (resp. positive p-order). But ord_p and ν_{L_t} are each either nonnegative or positive wherever the other is, so we can also define $\mathcal{O}_{L_w}$ (resp. $\mathfrak{M}_{L_w}$) to be the set of members of L_w with nonnegative (resp. positive) L_t-order.

Suppose ord_p and ν_{L_t} have their domains extended maximally to L_s. Multiplication by e_{L_t} gives a bijective order-preserving correspondence between the image of the p-order function and the image of the L_t-order function. In particular, whereas one might expect a uniformizer ϖ_{L_w} which generates $\mathfrak{M}_{L_w}$ (or any generator of an ideal $I \subseteq \mathcal{O}_{L_w}$) to have to be defined in some strange fashion without the use of the p-order function or the p-adic absolute value, it is sufficient to take a member of the ideal with minimal L_t-order. Minimal L_t-order bijectively corresponds to minimal p-order.

For $0 \leq w \leq v \leq s$, the ramification index e_{L_v/L_w} was defined to be the unique natural number such that in the ring $\mathcal{O}_{L_v}$, the ideals $(\varpi_{L_w}^{e_{L_v/L_w}})$ and (ϖ_{L_v}) are equal. Recall the result that $ord_p(L_v) = \frac{1}{e_{L_v}}\mathbb{Z}$. We have a completely analogous result when we rescale the p-order:

Theorem 4.1. $\nu_{L_w}(L_v) = \frac{1}{e_{L_v/L_w}}\mathbb{Z}$.

Proof. We have $\nu_{L_w}(L_v) = e_{L_w} ord_p(L_v) = e_{L_w} \frac{1}{e_{L_v}}\mathbb{Z} = \frac{1}{e_{L_v/L_w}}\mathbb{Z}$. $\square$

5 The Discriminant and the Resolvent

Let L be an m-dimensional extension of K, where K is a finite dimensional extension of $\mathbb{Q}_p$. Lemma 3.8 and Theorem 3.9 can be generalized with no difficulty to yield:

Theorem 5.1. *$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.*

Let $\sigma_1, ..., \sigma_m$ be all the embeddings of L into a fixed algebraic closure $\overline{\mathbb{Q}_p}$ containing K. If $a_1, ..., a_m$ is any collection of m elements of $\mathcal{O}_L$, we define the *discriminant* of $a_1, ..., a_m$ to be Δ^2, where Δ is the determinant of the matrix:

$$\begin{pmatrix} \sigma_1(a_1) & \cdots & \sigma_1(a_m) \\ \vdots & \vdots & \vdots \\ \sigma_m(a_1) & \cdots & \sigma_m(a_m) \end{pmatrix}$$

Since switching rows or columns changes the determinant by a factor of -1, the discriminant of an unordered collection of m members of $\mathcal{O}_L$ is well defined up to parity.

An *integral basis* of $\mathcal{O}_L$ over $\mathcal{O}_K$ is a basis for $\mathcal{O}_L$ over $\mathcal{O}_K$, i.e. a collection of elements in $\mathcal{O}_L$ of which every member of $\mathcal{O}_L$ is a unique $\mathcal{O}_K$-linear combination.

Lemma 5.2. *There exists an integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$, and the number of elements in any integral basis is m.*

Proof. See [6], pg. 6 - 7. □

Now let $v_1, ..., v_m$ be an integral basis for $\mathcal{O}_L$ over $\mathcal{O}_K$. We define the *field discriminant* $Disc(L/K)$ to be the ideal in $\mathcal{O}_L$ generated by $Disc(v_1, ..., v_m)$.

This notion is well defined regardless of a choice of integral basis.

Theorem 5.3. *Suppose $v_1, ..., v_n$ and $w_1, ..., w_m$ are integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$. Then $Disc(v_1, ..., v_n)$ and $Disc(w_1, ..., w_n)$ have the same p-order.*

Proof. Each w_i is an $\mathcal{O}_K$ linear combination of $v_1, ..., v_m$, so where $W = [w_1 \cdots w_m]^t$ and $V = [v_1 \cdots v_m]^t$, we have a matrix $X \in ML_m(\mathcal{O}_K)$ with $W = XV$. Similarly we have a matrix $X' \in ML_m(\mathcal{O}_K)$ going the other way, as $V = X'W$. Then $X' = X^{-1}$ (in particular X is invertible in $ML_m(\mathcal{O}_K)$) whence $Det(X)$ is a unit in $\mathcal{O}_K$. Moreover, for any linear combination of $v_1, ..., v_m$ forming a basis element w_i, the same linear combination of $\sigma_j(v_1), ..., \sigma_j(v_m)$ will equal $\sigma_j(w_i)$ for any $1 \le j \le m$, from which it follows that $Disc(w_1, ..., w_m) = Det(X)^2 Disc(v_1, ..., v_m)$. But then these two discriminants have the same p-order (or K-order, L-order, it doesn't matter), so being associates in $\mathcal{O}_L$ they must generate the same principal ideal. □

Where f is a polynomial in any field, and $r_1, ..., r_{deg(f)}$ are all its roots (with multiplicity) in some fixed algebraic closure of the field, we have the *polynomial discriminant* $Disc(f)$ defined as $\prod\limits_{i \neq j} (r_i - r_j)$.

A *power integral basis* of $\mathcal{O}_L$ over $\mathcal{O}_K$ is an integral basis of the form $1, a, a^2, ..., a^{m-1}$.

Theorem 5.4. *Suppose L is Galois over K. If $1, a, a^2, ..., a^{m-1}$ is a power integral basis for $\mathcal{O}_L$ over $\mathcal{O}_K$ and $\mu \in K[X]$ is the minimal polynomial of a over K (note that μ will be in $\mathcal{O}_K[X]$ by Theorem 5.1), then the field discriminant $Disc(L/K)$ and the ideal in $\mathcal{O}_L$ generated by $Disc(\mu)$ are equal.*

Proof. For every $\sigma_i \in Aut(L/K)$, we have $\sigma_i(a^j) = \sigma_i(a)^j$. Now the matrix Δ

$$\begin{pmatrix} 1 & \sigma_1(a) & \sigma_1(a)^2 & \cdots & \sigma_1(a)^m \\ \vdots & \vdots & & \vdots & \\ 1 & \sigma_m(a) & \sigma_m(a)^2 & \cdots & \sigma_m(a)^m \end{pmatrix}$$

is such that the ideal generated by $Det(\Delta)^2$ is $Disc(K/F)$. But the determinant of Δ is $\prod_{i<j}(\sigma_i(a) - \sigma_j(a))$, whence $Det(\Delta)^2 = \prod_{i \neq j}(\sigma_i(a) - \sigma_j(a))$. But $\sigma_1(a), ..., \sigma_n(a)$ are precisely all the roots of μ, so this latter square is just $Disc(\mu)$. □

Theorem 5.5. *Where $a_1, ..., a_m$ are, counting multiplicity, all the roots of a polynomial f, then $Disc(f) = \prod_{i=1}^{m} f'(a_i)$.*

Proof. Since $f(x) = \prod_{i=1}^{m}(x - a_i)$, we have $f'(x) = \sum_{j=1}^{m}\prod_{i \neq j}(x - a_i)$, whence for each root a_t we have $f'(a_t) = \prod_{i \neq t}(a_t - a_i)$.

Then $Disc(f) = \prod_{i \neq j}(a_i - a_j) = \prod_{i=1}^{m}\prod_{j \neq m}(a_i - a_j) = \prod_{i=1}^{m} f'(a_i)$. □

Let $f \in \mathbb{Z}_p[X]$ be monic and irreducible over $\mathbb{Q}_p[X]$ with $A = \{\alpha_1, ..., \alpha_n\}$ the set of all its roots. Let L be a splitting field of f over $\mathbb{Q}_p$, and $G = Aut(L/\mathbb{Q}_p)$.

Now any subgroup H of S_n acts on $\mathbb{Q}_p[X_1, ..., X_n]$, the action given by $\sigma h(x_1, ..., x_n) = h(x_{\sigma(1)}, ..., x_{\sigma(n)})$. Thus for any polynomial h in n ordered indeterminates we may talk about the stabilizer S_H of h in H. It is of course possible to choose a set of coset representatives $s_1, ..., s_m$ of H/S_H such that $\{s_1 h, ..., s_m h\}$ is equal to the orbit of h.

We now define the *resolvent* of f with respect to h in H, denoted $R_H(h, f)(x)$, to be the polynomial $\prod_{i=1}^{m}(x - s_i h(\alpha_1, ..., \alpha_n))$. The coefficients of $R_H(h, f)$ are fixed by any member of H, and hence by any member of G, whence $R_H(h, f) \in \mathbb{Q}_p[X]$.

Theorem 5.6. *$R(h, f)$ has a root in $\mathbb{Q}_p$ if and only if G is contained in a conjugate of S_H as a subgroup of S_n.*

From the preceding theorem we obtain a general method to find the Galois group of an irreducible $f \in \mathbb{Z}_p[X]$:

For each maximal transitive subgroup M of S_n, let $h \in \mathbb{Z}[X_1, ..., X_n]$ be a polynomial whose stabilizer is M. Compute $R_{S_n}(h, f)$ and check whether it has ax root in $\mathbb{Q}_p$. If it does, G will be contained in a conjugate of M and we can move on. If it does not, check the next maximal transitive subgroup of S_n.

If none of the resolvents we calculated in terms of the maximal transitive subgroups of S_n have roots in $\mathbb{Q}_p$, we can conclude that $G = S_n$.

If, however, G was found to be contained in some conjugate (liz., isomorphic copy) of M, then repeat the process for M: for each maximal transitive subgroup N of M, find a polynomial $h \in \mathbb{Z}[X_1, ..., X_n]$ whose stabilizer in M is N. Compute $R_M(h, f)$ and check whether it has a root in $\mathbb{Q}_p$. If it does, G will be contained in a conjugate of N. If it does not, check the next maximal transitive subgroup of M.

If none of the resolvents we calculated in terms of the maximal transitive subgroups of M have roots in $\mathbb{Q}_p$, we can conclude $G = M$.

Repeating this process we find smaller and smaller candidates for G until we find it.

This process would theoretically allow us to compute any Galois group. Unfortunately, this method is not very practical, as we must find the roots of the polynomial which is in general pretty hard. However, there is another method, using *linear resolvents* which is not guaranteed to give us a complete solution for the Galois group, but allows us to rule out several possibilties.

A linear resolvent is a resolvent with respect to a polynomial of the form $c_1x_1 + ... + c_rx_r \in \mathbb{Z}[X_1, ..., X_r, ..., X_n]$.

Now for $r \geq 2$, let W_r be the set of subsets of $\{1, 2, ..., n\}$ with cardinality r. S_n acts on W_r, the action given by $\sigma\{a_1, a_2, ..., a_r\} = \{\sigma(a_1), \sigma(a_2), ..., \sigma(a_r)\}$.

Every subgroup of S_n, as H, also acts on W_r, and induces a partition thereon, as S, T, V etc. where $S \cup T \cup V \cdots = W_r$ and $\binom{n}{r} = |W_r| = |S| + |T| + |V| + ...$ We then define the *r-partition length* of H in S_n to be the multiset $(|S|, |T|, |V|, ...)$.

If a resolvent has multiple roots, it is possible to apply a *Tschirnhausen transformation* to obtain a new resolvent which has distinct roots (in particular, the resolvent will be squarefree as a product of irreducibles). For more information about Tschirnhausen transformations, see (some source).

Theorem 5.7. *For $r \geq 2$, let R be the linear resolvent $R_{S_n}(x_1 + ... + x_r, f)$. If R has a multiple root, apply a Tschirnhausen transformation to R so that all its roots are distinct, and relabel R. Factor R in $\mathbb{Q}_p[X]$ as a product of irreducibles, as $\mu_1 \cdots \mu_t$. Then the r-partition length of G is $(\deg(\mu_1), ..., \deg(\mu_t))$.*

Thus by calculating, for various (small) r the r-partition length of the transitive subgroups of S_n and the factorization of linear resolvents of f with respect to $x_1 + ... + x_r$, it is possible to rule out several Galois groups with different partition lengths.

6 Unramified Extensions

In this section we show that for every positive integer n there is a unique unramified extension of $\mathbb{Q}_p$ having degree n.

Theorem 6.1. *Let K be a finite dimensional extension of $\mathbb{Q}_p$ with residue field k. There is a bijection*

$$\{L/K \text{ finite and unramified}\} \longleftrightarrow \{l/k \text{ finite}\}$$

where $L \mapsto l = \mathcal{O}_L/\mathfrak{m}_L$. Additionally this satisfies

1. *If L_1 and L_2 are finite unramified extensions of K with residue fields l_1 and l_2 then $L_1 \subseteq L_2$ if and only if $l_1 \subseteq l_2$.*
2. *$\mathrm{Aut}(L/K) \cong \mathrm{Aut}(l/k)$ under $\sigma \mapsto \sigma|_{\mathcal{O}_L}$.*

Proof. Let $p = \mathrm{char}(k)$. The proof is broken into several steps.

Step 1: Let m be a positive integer not divisible by p. Then the irreducible factors of $x^m - 1$ in $k[x]$ are the reductions modulo $\mathfrak{M}_K$ of the irreducible factors of $x^m - 1$ in $\mathcal{O}_K[x]$.

Proof of Step 1: Write $x^m - 1 = g_1^{n_1}(x)...g_r^{n_r}(x) \in \mathcal{O}_K[x]$ for irreducible $g_1(x), ..., g_r(x)$. Let $\overline{g_i(x)}$ be the reduction of $g_i(x)$ modulo $\mathfrak{m}_K$. We need to show that $\overline{g_i(x)}$ is still irreducible. Note that since $\gcd(p, m) = 1$, $x^m - 1$ is separable in $k[x]$ and hence so is each $\overline{g_i}$.

Let $\overline{f} \in k[x]$ be a monic irreducible factor of $\overline{g_i}$ and let $f \in \mathcal{O}_k[x]$ be a monic polynomial such that f modulo $\mathfrak{m}_K$ is $\overline{f}$. Note that f is irreducible because otherwise $\overline{f}$ would be reducible. Let α be any root of f and set $E = K(\alpha)$. We have

$$[E : K] = \deg(f) = \deg(\overline{f}) \leq \deg(\overline{g_i}) = \deg(g_i).$$

We know that $\overline{f}(\overline{\alpha}) = 0$ so $\overline{g_i}(\overline{\alpha}) = 0$ where we think of $\overline{\alpha}$ as being in the residue field of E. Now because $\overline{g_i}$ is separable, we can apply Hensel's lemma to get a root $\beta \in \mathcal{O}_E$ of g_i. This gives $K(\beta) \subseteq E$. We have

$$\deg(g_i) = [K(\beta) : K] \leq [E : K] \leq \deg(g_i).$$

Hence $\deg(g_i) = [E : K]$. Thus $\deg(\overline{f}) = \deg(\overline{g_i})$, so $\overline{g_i}$ is irreducible.

Step 2: Let l/k be a separable extension of degree n. Then there exists a unique unramified extension K_n/K that is finite and has residue field l.

Proof of Step 2: Since l is finite there exists $\overline{\alpha}$ such that $l = k(\overline{\alpha})$. Let $m = |l| - 1$. Then $\overline{\alpha}$ is a root of $x^m - 1 \in k[x]$ since $l^\times$ is a cyclic group of order m. Let $\overline{f}$ be the minimal polynomial of $\overline{a}$ over k. This means $\overline{f}$ is some irreducible factor of $x^m - 1$ in $k[x]$. By step 1 there is some irreducible factor $f \in \mathcal{O}_K[x]$ of $x^m - 1$ which reduces to f modulo $\mathfrak{M}_K$. Let β be any root of f and set $K_n = K(\beta)$. Then

$$[K_n : K] = \deg(f) = \deg(\overline{f}) = [l : k] = n.$$

Because $\overline{\beta} \in \mathcal{O}_{K_n}/\mathfrak{m}_k$ then $k(\overline{\beta}) \subseteq \mathcal{O}_{K_n}/\mathfrak{M}_k$. It follows that

$$n \geq f(K_n/K) = [\mathcal{O}_{K_n}/\mathfrak{m}_k : k] \geq [k(\overline{\beta}) : k] = n.$$

Hence $f(K_n/K) = n$ so K_n/K is unramified and $l = \mathcal{O}_{K_n}/\mathfrak{m}_k$ since they are both extensions of k of the same degree.

Now we just need to prove uniqueness. Suppose L/K is such that the residue field of L is l. Since $\overline{f}$ has a a root $\overline{\alpha} \in l$ and $\overline{f}$ is separable then f has a root $\alpha \in O_L$ by Hensel's lemma. Thus $K(\alpha) \subseteq L$ and $K(\alpha) \cong K_n$. If L is unramified, then $n = [L : K]$, thus $L = K(\alpha) \cong K_n$. This completes the uniqueness part.

A similar argument will give us part 1 of the theorem. Let L_1, L_2 be finite unramified extensions of K with residue fields l_1, l_2 respectively. First suppose $L_1 \subseteq L_2$. It is straightforward to show that $l_1 \subseteq l_2$: define the map $\phi : \mathcal{O}_{L_1} \to \mathcal{O}_{L_2}/\mathfrak{M}_{L_2}$ by $x \mapsto x + \mathfrak{M}_{L_2}$. Then since $\mathfrak{M}_{L_1} \subseteq \mathfrak{M}_{L_2}$ we get that $\mathfrak{M}_{L_1} \subseteq \ker(\phi)$. Now suppose $x \in \mathcal{O}_L$ but $x \notin \mathfrak{M}_{L_1}$. Then x is a unit, so $x \notin \mathfrak{M}_{L_2}$. Hence $x \notin \ker(\phi)$, so $\ker(\phi) = \mathfrak{M}_{L_1}$. By the the first isomorphism theorem for rings, we can conclude

$$\mathrm{im}(\phi) \cong (\mathcal{O}_{L_1}/\mathfrak{M}_{L_1}).$$

This gives us $l_1 \subseteq l_2$.

To go the other direction, suppose $l_1 \subseteq l_2$. Then there exist $\overline{\alpha}, \overline{\beta} \in l_2$ such that $l_1 = k(\overline{\alpha})$ and $l_2 = k(\overline{\beta})$. Let $\overline{f_1}, \overline{f_2}$ be the minimal polynomials of $\overline{a}$ and $\overline{\beta}$ respectively. By Hensel's lemma we can find $\alpha, \beta \in \mathcal{O}_{L_2}$ such that $f_1(\alpha) = 0$ and $f_2(\beta) = 0$. Since f_1 and f_2 are necessarily irreducible, we get that $[L_1 : K] = [K(\alpha) : K] = \deg(f_1)$ and $[L_2 : K] = [K(\beta) : K] = \deg(f_2)$. Furthermore these two extensions are unramified, and by the uniqueness of such unramified extensions we get that $L_1 \cong K(\alpha)$ and $L_2 \cong K(\beta)$. Clearly since $L_2 \cong K(\beta)$ then $\alpha \in K(\beta)$. It follows that $K(\alpha) \subseteq K(\beta)$, so $L_1 \subseteq L_2$.

Step 3: Let l/k be a finite separable extension of degree n. Then $\mathrm{Aut}(K_n/K) \cong Aut(l/k)$

Proof of Step 3: Let f and $\overline{f}$ be as in step 2. By Hensel's lemma any root of $\overline{f}$ in l lifts to a root of f in $\mathcal{O}_{K_n}$. Let $\alpha_1, ..., \alpha_n$ be the roots of f and let $\overline{\alpha}_1, ...\overline{\alpha}_n$ be the roots of $\overline{f}$ such that $\overline{\alpha}_i$ is the reduction of α_i modulo $\mathfrak{M}_{K_n}$. Consider the map $\mathrm{Aut}(K_n/K) \to \mathrm{Aut}(l/k), \sigma \mapsto \{$ the image of σ in $\mathrm{Aut}(l/k)\}$. To see that this is well-defined, suppose $x \equiv y \pmod{\mathfrak{M}_L}$. Then $x - y \in \mathfrak{M}_L$. Because σ preserves the valuation, then $\sigma(x) - \sigma(y) \in \mathfrak{M}_L$. Hence $\overline{\sigma}(\overline{x}) = \overline{\sigma}(\overline{y})$ if $\overline{x} = \overline{y}$. Now let $\sigma \in \mathrm{Aut}(K_n/K)$ such that $\sigma \neq \mathrm{id}$. Then there exist some i, j with $i \neq j$ such that $\sigma(\alpha_i) = \sigma(\alpha_j)$. This is because $K_n = K(\alpha_p)$ for some $1 \leq p \leq n$ and such a σ is uniquely determined by where it sends α_j. Then $\overline{\sigma}(\overline{\alpha}_i) = \overline{\sigma(\alpha_i)} = \overline{\alpha}_i \neq \overline{a}_j$. Hence $\overline{\sigma} \neq \mathrm{id}$. So the kernel of the map $\mathrm{Aut}(K_n/K) \to \mathrm{Aut}(l/k)$ is $\{\mathrm{id}\}$. Thus this map is injective. Now since both Galois groups have order n, we can conclude that this map is a bijection. It is clear that this map is a homomorphism, so we can now conclude the two Galois groups are isomorphic. □

Lemma 6.2. *Let K be a finite extension of $\mathbb{Q}_p$. If L_1, L_2 are finite dimensional extensions of K with L_1 an unramified extension of K, then L_1L_2 is an unramified extension of L_2.*

Proof. Let l_1, l_2 be the residue fields of L_1, L_2 and let l' be the residue field of L_1L_2. Set $l_1 = k(\bar{\alpha})$ for some $\alpha \in \mathcal{O}_{L_1}$. Let $f \in L_1[X]$ be the minimal polynomial of α over K, with $\bar{f} \in k[X]$. Note $[l : k] \leq \deg(\bar{f}) = \deg(f) = [K(\alpha) : K] \leq [L_1 : K]$, which is equal to $[l_1 : k]$ since L/K is unramified. Thus $L_1 = K(\alpha)$ and $\bar{f} \in k[X]$ is the minimal polynomial of $\bar{\alpha}$ over K.

This gives $L_1L_2 = K(\alpha)L_2 = L_2(\alpha)$. It is left to show $L_1L_2/L_2(\alpha)$ is unramified. Let $g \in L_2[X]$ be the minimal polynomial of α over L_2. Since g divides f, $\bar{g}$ divides $\bar{f}$, so $\bar{g}$ is separable and irreducible by Hensel's Lemma.

Thus for $l' = \mathcal{O}_{L_1L_2}/\mathfrak{M}_{L_1L_2}$, $[l' : l_2] \leq [L_2(\alpha) : L_2] = \deg(g) = \deg(\bar{g}) = [l_2(\alpha) : l_2] \leq [l' : l_2]$. Then $[l' : l_2] = [L_2(\alpha) : L_2]$, so we are done. □

Corollary 6.3. *A compositum of finitely many unramified extensions of $\mathbb{Q}_p$ is an unramified extension of $\mathbb{Q}_p$.*

Proof. Obvious from the preceding lemma, and from the multiplicativity of ramification indices. □

7 Totally Ramified Extensions

Let K be a finite dimensional extension of $\mathbb{Q}_p$, and ϖ_K a uniformizer for $\mathcal{O}_K$. A polynomial $a_0 + a_1x + ... + a_mx^m \in \mathcal{O}_K[X]$ is called an *Eisenstein polynomial* if $\varpi \nmid a_m$, $\varpi \mid a_1, ..., a_{m-1}$, and $\varpi^2 \nmid a_0$. This generalizes the "Eisenstein criterion," seen in abstract algebra or number theory, which can determine if a polynomial in $\mathbb{Q}[X]$ is irreducible. Indeed, any Eisenstein polynomial is irreducible in $K[X]$ by the same argument. The notion of adjoining a root of an Eisenstein polynomial to $\mathbb{Q}_p$ will be very useful in classifying totally ramified extensions. An extension L/K is called an *Eisenstein extension* if L can be obtained by adjoining a root of an Eisenstein polynomial of $\mathcal{O}_K[X]$ to K.

As an example of the previous definition, note that the polynomial $x^2 - 3 \in \mathbb{Z}_3[x]$ is Eisenstein. Hence the extension $\mathbb{Q}_3(\alpha)/\mathbb{Q}_3$ where α is a root of $x^2 - 3$ is an Eisenstein extension. Now we show that any Eisenstein extension is totally ramified.

Theorem 7.1. *Suppose L/K is Eisenstein. Then L is totally ramified over K.*

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathcal{O}_K[x]$ be an Eisenstein polynomial, and $\alpha \in \mathcal{O}_K$ a root of f such that $L = K(\alpha)$. Let $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$ be all the roots of f, ϖ_K a uniformizer of K, and ϖ_L a uniformizer of L. It is required to show that $e_{L/K} = 1$, where $|\varpi_L^{e_{L/K}}| = |\varpi_K|$. Since all the roots of f have the same absolute value, $|\alpha|^n = \prod_{i=1}^{n} |\alpha_i| = |a_0|$, with $|a_0| = |\varpi_K|$ by hypothesis. Since $\alpha \in \mathcal{O}_L$, there exists some $m \in \mathbb{N}$ with $|\varpi_L|^m = |\alpha|$. Then $|\varpi_K|^{\frac{m}{e_{L/K}}} = |\varpi_L|^m = |\alpha| = |\varpi_K|^{\frac{1}{n}}$, or $mn = e_{L/K}$. But $e_{L/K} \leq n$, so we must conclude $m = 1$, i.e. $n = e_{L/K}$. □

Theorem 7.2. *If a finite extension L/K is totally ramified then L/K is Eisenstein.*

Proof. Let L/K be totally ramified with $[L : K] = n$. Let ϖ_L be a uniformizer of L. Consider the intermediate field $L_1 = K(\varpi_L)$. Since $L/\mathbb{Q}_p$ is totally ramified then $L_1/\mathbb{Q}_p$ is totally ramified. Let ϖ_{L_1} be a uniformizer of L_1. Since $\varpi_L \in L_1$ it follows that $|\varpi_{L_1}| = |\varpi_L|$. Because L/K is totally ramified then $|\varpi_K| = |\varpi_L|^n$. We also have $|\varpi_K| = |\varpi_{L_1}|^{[L_1:K]} = |\varpi_L|^{[L_1:K]}$. Hence $[L_1 : K] = n$, so $L_1 = L$.

Now let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathcal{O}_K[x]$ be the minimal polynomial of ϖ_L over K. Let $\varpi_L = \varpi_1, ..., \varpi_n$ be the roots of f. All these roots have absolute value equal to $|\varpi_L| < 1$. Hence $|a_i| < 1$ since the a_i's are symmetric polynomials in the ϖ_i. So $a_i \in \mathfrak{M}_K$. Also, since $L/\mathbb{Q}_p$ is totally ramified,

$$|a_0| = \prod_{i=1}^{n} |\varpi_i| = |\varpi_L|^n = |\varpi_K|.$$

Hence a_0 is not divisible by ϖ_K^2, so f is Eisenstein. □

Corollary 7.3. *A finite extension L/K is totally ramified if and only if L/K is Eisenstein.*

Thus in order to classify totally ramified extensions of $\mathbb{Q}_p$, we need only consider those extensions obtained by adjoining a root of an Eisenstein polynomial to $\mathbb{Q}_p$.

We will see toward the end of this section that it is always possible to split up a finite extension $L/\mathbb{Q}_p$ into an unramified extension and then a totally ramified extension $\mathbb{Q}_p \subseteq L_{\text{ur}} \subseteq L$. The unramified extension is easy to classify, since there is a unique unramified extension of every degree. Thus, to classify extensions of $\mathbb{Q}_p$ it is left to focus on the totally ramified extensions of the unramified extensions of $\mathbb{Q}_p$. To study these extensions, we will use a very useful tool known as Krasner's Lemma.

Krasner's Lemma 7.4. *Let K be a finite extension of $\mathbb{Q}_p$, and $\overline{K}$ an algebraic closure of K. If there exists $\alpha, \beta \in K$ such that $|\alpha - \beta| < |\alpha - \sigma(\alpha)|$ for all $\sigma \in Aut(\overline{K}/K)$ such that $\sigma(\alpha) \neq \alpha$, i.e., β is closer to α than any of α's nontrivial Galois conjugates, then $K(\alpha) \subseteq K(\beta)$.*

Proof. Take $\sigma \in \text{Aut}(\overline{K}/K)$ such that $\sigma(\beta) = \beta$. We would like to show that $\sigma(\alpha) = \alpha$, in which case we would have that $\text{Aut}(\overline{K}/K(\beta)) \subseteq \text{Aut}(\overline{K}/K(\alpha))$ and the Fundamental Theorem of Galois Theory would give us that $K(\alpha) \subseteq K(\beta)$.

By the previous lemma,

$$\begin{aligned} |\alpha - \beta| &= |\sigma(\alpha - \beta)| \\ &= |\sigma(\alpha) - \sigma(\beta)| \\ &= |\sigma(\alpha) - \beta| \end{aligned}$$

Now,

$$\begin{aligned}|\sigma(\alpha)-\alpha| &= |(\sigma(\alpha)-\beta)+(\beta-\alpha)| \\ &\leq \max\{|\sigma(\alpha)-\beta|,|\alpha-\beta|\}.\end{aligned}$$

Since $|\sigma(\alpha)-\beta| = |\alpha-\beta|$, we must have that $|\sigma(\alpha)-\alpha| \leq |\alpha-\beta|$. However, β is closer to α than any of α's nontrivial Galois conjugates, so σ must act trivially on α, i.e. $\sigma(\alpha)=\alpha$. $\square$

Definition 7.5. *For α,$\beta \in \overline{K}$, $\underline{\beta \text{ belongs to } \alpha}$ if $|\alpha-\beta| < |\sigma(\alpha)-\alpha|$ for all $\sigma \in Gal(\overline{K}/K)$.*

Krasner's Lemma says if β belongs to α, then $K(\alpha) \subseteq K(\beta)$.

We now define a metric on $K[X]$. For $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$, we define $\|f\|$ to be $\max_i |a_i|$.

Lemma 7.6. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ be irreducible and take $\alpha \in \overline{K}$ such that $f(\alpha) = 0$. Then, there exists a constant $c_f > 0$ such that if $g(x) \in K[x]$ with $\|g - f\| \leq c_f$, then $g(x)$ has a root β that belongs to α. Also, $g(x)$ is irreducible,* $\deg g(x) = \deg f(x)$*, and $K(\alpha) = K(\beta)$.*

Proof. Pick c_f such that

$$c_f < \min(1, \|f(x)\|) \tag{1}$$

$$c_f < \min_{\sigma(\alpha)\neq\alpha} (c_1^{-1}|\sigma(\alpha)-\alpha|_p^n) \tag{2}$$

where $c_1 = \max_{\substack{0\leq m\leq n-1\\ 0\leq j\leq n-1}} \|f(x)\|^{\frac{m}{n-j}}$. Now, take $g(x) \in K[x]$ monic such that $\|g(x)-f(x)\| \leq c_f$. If $\deg g(x) \neq n$, then we have $\|g(x)-f(x)\| \geq 1$. However, since $c_f \leq 1$ by equation (1), we must have $\deg g(x) = n$

Now,

$$\begin{aligned}\|g(x)\| &= \|f(x) + (g(x)-f(x))\| \\ &\leq \max(\|f(x)\|, \|f(x)-g(x)\|) \\ &\leq \|f(x)\|\end{aligned}$$

where the first inequality comes from the non-archimedean absolute value, and the second inequality is because $\|g(x)-f(x)\| \leq c_f < \|f(x)\|$.

Write $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ and take $\beta_0 \in \overline{K}$ with $g(\beta_0) = 0$. Then,

$$\begin{aligned}|\beta_0^n| &= \left|\sum_{i=0}^{n-1} b_i \beta_0^i\right| \\ &\leq \max_{0\leq i\leq n-1} |b_i||\beta_0|^i.\end{aligned}$$

Let j be such that $|b_j||\beta_0|^j$ is maximal. So, $|\beta_0|^n \leq |b_j||\beta_0|^j$. Note $|\beta_0|^{n-j} \leq |b_j| \leq \|g(x)\|$; for if $\beta_0 \neq 0$ then we can divide through by β_0, and if $\beta_0 = 0$ this result is clearly true. As we saw earlier $\|g(x)\| \leq \|f(x)\|$, so if we take roots and combine the last two inequalities, we get $|\beta_0| \leq \|f(x)\|^{\frac{1}{n-j}}$.

Let $f(x) - g(x) = \sum_{m=0}^{n-1} c_m x^m$. Since $g(\beta_0) = 0$,

$$\begin{aligned}
|f(\beta_0)| &= |f(\beta_0) - g(\beta_0)| \\
&\leq \max_{0 \leq m \leq n-1} |c_m||\beta_0|^m \\
&\leq c_f \max_{0 \leq m \leq n-1} |\beta_0|^m \\
&\leq c_f \max_{0 \leq m \leq n-1} \|f(x)\|^{\frac{m}{n-j}} \\
&< \min_{\sigma(\alpha) \neq \alpha} |\sigma(\alpha) - \alpha|^n
\end{aligned}$$

where the last inequality comes from defining equation (2) of c_f.

Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$. So $|(\beta_0 - \alpha_1) \ldots (\beta_0 - \alpha_n)| = |f(\beta_0)| < \min_{\sigma(\alpha) \neq \alpha} |\sigma(\alpha) - \alpha|_p^n$. Suppose i minimizes $|\beta_0 - \alpha_i|$. Then, $|\beta_0 - \alpha_i| < |\sigma(\alpha) - \alpha|$ for all σ such that $\sigma(\alpha) \neq \alpha$

The group $\mathrm{Aut}(\overline{K}/K)$ acts transitively on the roots of irreducible polynomials, so there exists $\sigma_i \in \mathrm{Aut}(\overline{K}/K)$ such that $\sigma_i(\alpha_i) = \alpha$. Let $\beta_i = \sigma_i(\beta_0)$. Then, for all $\sigma \in \mathrm{Aut}(\overline{K}/K)$ such that $\sigma(\alpha) \neq \alpha$ we have

$$\begin{aligned}
|\beta_i - \alpha| &= |\sigma_i(\beta_i - \alpha)| \\
&= |\sigma_i(\beta_i) - \sigma_i(\alpha)| \\
&= |\beta_0 - \alpha_i| \\
&< |\sigma(\alpha) - \alpha|
\end{aligned}$$

So, β_i belongs to α. Krasner's Lemma gives $K(\alpha) \subseteq K(\beta_i)$. Since $f(x)$ is irreducible we have,

$$\begin{aligned}
\deg f(x) &= [K(\alpha) : K] \\
&\leq [K(\beta_i) : K[\\
&\leq \deg g(x).
\end{aligned}$$

Since $\deg f(x) = \deg g(x)$ we must have $K(\alpha) = K(\beta_i)$. □

Corollary 7.7. *Take $f(x), g(x), c_f$ as in the previous lemma. Then every root of $g(x)$ belongs to exactly one root of $f(x)$. So the roots of $f(x)$ generate the same extensions as the roots of $g(x)$.*

Proof. Let α be a root of $f(x)$ and let β be a root of $g(x)$, β's existence is guaranteed by the previous lemma. Let $\beta = \beta_1, \beta_2, \ldots, \beta_n$ be the roots of $g(x)$.

First, let's show every root of $g(x)$ belongs to at least one root of $f(x)$. Since $g(x)$ is irreducible, and the Galois group acts transitively on the roots of irreducible polynomials, there exists $\sigma_i \in \mathrm{Gal}(\overline{K}/K)$ such that $\sigma_i(\beta) = \beta_i$. So

$$\begin{aligned}
|\sigma_i(\alpha) - \beta_i| &= |\sigma_i(\alpha) - \sigma_i(\beta)| \\
&= |\alpha - \beta| \\
&< |\alpha_i - \alpha| \text{ for all i} \neq 1.
\end{aligned}$$

The last inequality is because β belongs to α and the collection of α_i's such that $i \neq 1$ is the collection of non-trivial Galois conjugates of α. So, β_i belongs to $\sigma_i(\alpha)$.

Now, suppose β belongs to α and $\alpha_k \neq \alpha$. We may write $\alpha_k = \tau(\alpha)$ for some $\tau \in \mathrm{Aut}(\overline{K}/K)$. By the non-Archimedean property, we get $|\tau(\alpha)-\alpha| \leq \max\{|\tau(\alpha)-\beta|, |\beta-\alpha|\}$. Since β belongs to α, we know $|\alpha-\beta| < |\tau(\alpha)-\alpha|$. Also, since β belongs to $\tau(\alpha)$ we have

$$\begin{aligned} |\tau(\alpha)-\beta| &< |\alpha-\tau^{-1}(\alpha)| \\ &= |\tau(\alpha-\tau^{-1}(\alpha))| \\ &= |\tau(\alpha)-\alpha| \end{aligned}$$

Thus we have $|\tau(\alpha)-\alpha| \leq \max\{|\tau(\alpha)-\beta|, |\beta-\alpha|\} < |\tau(\alpha)-\alpha|$. Thus, we can not have a root of $f(x)$ belonging to two roots of $g(x)$. Since we know that $\deg g(x) = \deg f(x)$ and both polynomials are irreducible and separable, we must have that each root of $g(x)$ belongs to one and only one root of $f(x)$. The facts about the field extensions follows from the previous lemma. □

Now, using these tools, we can show that there are only finitely many totally ramified (equivalently Eisenstein) extensions of K

Lemma 7.8. *There are only finitely many Eisenstein extensions of K having a fixed degree n.*

Proof. Let $A = \mathfrak{M}_K \times \cdots \times \mathfrak{M}_K \times (\mathfrak{M}_K \setminus \varpi\mathcal{O}_K)$, where ϖ is a uniformizer for $\mathcal{O}_K$ and there are $n-1$ copies of $\mathfrak{M}_K$. We have a bijection from A to the set of all Eisenstein polynomials of $\mathcal{O}_K[x]$ of degree n by mapping each n-tuple $(a_{n-1}, ..., a_0)$ to the polynomial $a_0 + ... + a_{n-1}x^{n-1} + x^n \in \mathcal{O}_K[X]$.

We can make A a metric space by defining $\|(a_{n-1}, \ldots, a_0)\| = \max\limits_i |a_i|$. This metric coincides with the product topology on A, and the aforementioned bijection gives a homeomorphism between A and the metric subspace $\{f \in K[X] : f \text{ is monic}, \deg(f) \leq n\}$. For $a \in A$ denote the corresponding polynomial by f_a.

For each $a \in A$ there exists a neighborhood $U_a \subseteq A$ such that if $b \in U_a$, then the roots of f_b and f_a generate the same extension, where $U_a = \{x \in A : \|x-a\| < c_{f_a}\}$ for c_{f_a} as defined in Lemma 3.

Now, $\mathfrak{M}_K$ is closed in $\mathcal{O}_K$, which is compact, so $\mathfrak{M}_K$ is compact. Note $\varpi^2\mathcal{O}_K = \{x \in \mathcal{M}_K : |x| < |\varpi|\}$, so $\varpi^2\mathcal{O}_K$ is open in $\mathfrak{M}_K$. Thus its complement, $\mathfrak{M}_K \setminus \varpi^2\mathcal{O}_K$ is a closed subset of the compact set $\mathfrak{M}_K$, so $\mathfrak{M}_K \setminus \varpi^2\mathcal{O}_K$ is compact. A product of compact spaces is compact, so A is compact. So $A = \cup U_{a_1} \cup \cdots \cup U_{a_s}$ for some $a_1, ..., a_s \in K$, and so all the Eisenstein extensions of K are generated by the roots of $f_{a_1}, \ldots, f_{a_s}$ □

Theorem 7.9. *If L is finite dimensional over $\mathbb{Q}_p$, let K be the composite of all the unramified extensions of $\mathbb{Q}_p$ contained in L. Then K is an unramified extension of $\mathbb{Q}_p$, and L is a totally ramified extension of K.*

Proof. See [3] pg. 39. □

Corollary 7.10. *For every $n \geq 1$, there are finitely many fields which are n dimensional over $\mathbb{Q}_p$.*

Proof. For every positive nonunit divisor d of n, there is exactly one unramified extension K_d of $\mathbb{Q}_p$ having dimension d. And by the previous theorem, there are only finitely many totally ramified extensions of K_d which have dimension n/d over K_d.

Since every n dimensional extension L of $\mathbb{Q}_p$ can be broken up into an unramified extension $K/\mathbb{Q}_p$ and a totally ramified extension L/K, the assertion is obvious. □

8 Tamely Ramified Degree Fourteen Extensions of $\mathbb{Q}_p$

For $n > 1$ and e a divisor of n not divisible by p, Awtrey cites a general method for counting up to isomorphism the number of n-dimensional extensions of $\mathbb{Q}_p$ which have ramification index e:

Fixing e determines the dimension $f = n/e$ of the residue field. Let $g = (e, p^f - 1)$. Since $\mathbb{Z}$ acts on $\mathbb{Z}/g\mathbb{Z}$ by multiplication, the latter group may be partitioned into orbits under multiplication by p. Then there are as many nonisomorphic n-dimensional extensions of $\mathbb{Q}_p$ having ramification index e as there are orbits.

When p is not 2 or 7, all degree 14 extensions of $\mathbb{Q}_p$ are tamely ramified. We give a count of the number of such extensions based on p being congruent to $1, 3, 5, 9, 11$ or 13 modulo 14.

We divide this count into cases based on the four possibilities for (e, f).

I . There is up to isomorphism only one unramified extension of $\mathbb{Q}_p$ for each degree n, so there is nothing to prove when $e = 1$.

II . If $e = 2$ and $f = 7$, we have $g = (2, p^7 - 1) = 2$. p being nonzero modulo 2, multiplication by p induces only two orbits of $\mathbb{Z}/g\mathbb{Z}$: $\{0\}$ and $\{1\}$, so there are two nonisomorphic degree 14 extensions of $\mathbb{Q}_p$ with ramification index 2.

III. If $e = 7$ and $f = 2$, we have $g = (7, p^2 - 1)$, so g will be 7 when $p^2 \equiv 1 \pmod 7$, and 1 otherwise.

When $p \equiv 3, 5, 9$ or 11 modulo 14 (and therefore modulo 7), p^2 is evidently not congruent to 1, so $g = 1$. But then $\mathbb{Z}/g\mathbb{Z}$ is the trivial group, so multiplication by p induces only one orbit, yielding up to isomorphism only one extension.

When $p \equiv 1$, we have $g = 7$. But then multiplication by p puts each element of $\mathbb{Z}/g\mathbb{Z}$ into its own orbit, yielding 7 extensions.

Finally when $p \equiv 13$, we have $p \equiv -1 \pmod 7$ and $g = 7$. Multiplication by p induces the orbits $\{0\}$; $\{1, 6\}$; $\{2, 5\}$; $\{3, 4\}$ of $\mathbb{Z}/g\mathbb{Z}$, so we have 4 extensions.

IV. If $e = 14$ and $f = 1$, $g = (14, p - 1)$. When p is of the form $14k + 1$, g is 14. Then multiplication by p sorts the elements of $\mathbb{Z}/g\mathbb{Z}$ into trivial orbits, giving 14 extensions.

When p is of the form $14k$ plus $3, 5, 9, 11$ or 13, g is clearly equal to 2. By the same reasoning in II above, there are only 2 extensions.

Putting the above material together we deduce:

Theorem 8.1. *The number of nonisomorphic degree* 14 *extensions of* $\mathbb{Q}_p$ *is* 24 *when* $p \equiv 1$ *(mod* 14*),* 6 *when* $p \equiv 3, 5, 9$ *or* 11*, and* 8 *when* $p \equiv 13$.

The subcase where p is congruent to unity modulo the degree of the extension merits special attention. When n is of the form $2q$ for some odd prime q, and p is a prime number $\equiv 1 \pmod{2q}$, it is easy to see that the exact same arguments as above give us the following: up to isomorphism the number of $2q$-dimensional extensions of $\mathbb{Q}_p$ is $1 + 2 + q + 2q$.

More generally fixing a prime number p, we say that a natural number n is *p-adically perfect* if up to isomorphism the number of n-dimensional extensions of $\mathbb{Q}_p$ is $\sum_{d|n} d$.

It has been observed that there are many more wildly ramified extensions up to isomorphism than there are tamely ramified. It seems apparent that when p divides n, the number of degree n extensions of $\mathbb{Q}_p$ up to isomorphism should be greater than $\sum_{d|n} d$. Exact formulas (source) are known detailing the number of extensions up to isomorphism of $\mathbb{Q}_p$ of a fixed degree and ramification index, but working with these formulas to obtain a suitable lower bound on the number of extensions up to isomorphism in the wildly ramified case has been difficult. For the time being, all that can be done is to state the following conjecture:

Conjecture 8.2. *If n is p-adically perfect, then p cannot divide n.*

The following theorem along with the previous conjecture would completely characterizes p-adically perfect numbers:

Theorem 8.3. *Suppose p does not divide n. Then n is p-adically perfect if and only if $p \equiv 1 \pmod{n}$.*

Proof. First suppose $p \equiv 1 \pmod{n}$. Let e be any divisor of n. We have $g = (e, p^{n/e} - 1) = e$ since $p^{n/e}$ is congruent to unity modulo n, and therefore modulo e. But also $p \equiv 1 \pmod{e}$, so multiplying all the elements of $\mathbb{Z}/g\mathbb{Z}$ by p only sorts each element into its own orbit.

Thus there are e nonisomorphic n-dimensional extensions of $\mathbb{Q}_p$ with ramification index e, meaning there are $\sum_{e|n} e$ nonisomorphic extensions in total.

Conversely suppose n is p-adically perfect. Resolve n into prime factors, as $A^\alpha B^\beta C^\gamma$ etc.

Now for each divisor d of n, the number of orbits of $\mathbb{Z}/g\mathbb{Z}$ where $g = (d, p^{n/d} - 1)$ is $\leq g$, which is $\leq d$. Thus for n to be p-adically perfect there must be exactly d nonisomorphic degree n extensions of $\mathbb{Q}_p$ with ramification index d. Otherwise the sum over $d \mid n$ of the number of nonisomorphic extensions with ramification index d will be strictly less than $\sum_{d|n} d$.

For this to happen, we must first have $g = d$. Second, multiplication of $\mathbb{Z}/g\mathbb{Z}$ by p must sort each element into its own orbit, i.e. p must be congruent to unity modulo $d = g$.

Then $p \equiv 1$ modulo $A^\alpha, B^\beta, C^\gamma$ etc. and hence modulo their product n. $\square$

When $p \equiv -1$, a similar but more complicated result can be deduced:

Theorem 8.4. *If p is an odd prime congruent to $-1 \pmod{n}$ with n even, then the number of n dimensional extensions of $\mathbb{Q}_p$ up to isomorphism is*

$$\sum_{\substack{d|n \\ ord_2(d) < ord_2(n)}} \left\lceil \frac{d+1}{2} \right\rceil + \sum_{\substack{d|n \\ ord_2(d) = ord_2(n)}} 2$$

.

Proof. Since p is odd, n is even, so we may write $n = 2^e p_1^{e_1} \cdots p_s^{e_s}$. Let d be any divisor of n with $ord_2(d) < e$. Then $g = (d, p^{n/d} - 1)$ is equal to d since n/d is even, ensuring $p^{n/d} \equiv (-1)^{n/d} = 1 \pmod{n}$ and therefore modulo d. Also $p \equiv -1 \pmod{d}$, so multiplication by p sorts $\mathbb{Z}/g\mathbb{Z}$ into the orbits $\{0\}$; $\{1, d-1\}$; $\{2, d-2\}$ etc.

Thus there are $\frac{d+1}{2}$ orbits if d is odd and $\frac{d}{2} + 1$ orbits if d is even.

Now let d be any divisor of n with $ord_2(d) = e$. Then n/d is odd, meaning $p^{n/d} \equiv (-1)^{n/d} = -1$ modulo n, and therefore modulo any odd prime p_i dividing n. We can then conclude that d and $p^{n/d} - 1$ do not have any odd prime divisors in common. On the other hand, $p^{n/d} \equiv (-1)^{n/d} = -1 \pmod{2^e}$, and therefore modulo 2^k for any $k \leq e$. But $-1 \equiv 1 \pmod{2^k}$ if and only if $k = 1$, so we can conclude that $g = (d, p^{n/d} - 1)$ is equal to 2.

From the fact that p itself is $1 \pmod{2}$, we can conclude that multiplication by p induces two orbits of $\mathbb{Z}/g\mathbb{Z}$.

Putting this all together, we see that the number of n-dimensional extensions of $\mathbb{Q}_p$ up to isomorphism is

$$\sum_{\substack{d|n \\ ord_2(d)=0}} \frac{d+1}{2} + \sum_{\substack{d|n \\ 1\le ord_2(d)<ord_2(n)}} \left(\frac{d}{2}+1\right) + \sum_{\substack{d|n \\ ord_2(d)=ord_2(n)}} 2$$

But

$$\sum_{\substack{d|n \\ ord_2(d)=0}} \frac{d+1}{2} + \sum_{\substack{d|n \\ 1\le ord_2(d)<ord_2(n)}} \left(\frac{d}{2}+1\right) = \sum_{\substack{d|n \\ ord_2(d)<ord_2(n)}} \left\lceil \frac{d+1}{2} \right\rceil$$

. □

Theorem 8.5. *If in the previous theorem n is odd, then up to isomorphism the number of n dimensional extensions of $\mathbb{Q}_p$ is the number of divisors of n.*

Proof. Let d be any nonunit divisor of n. For every nonunit divisor d_1 of d, from $p \equiv -1 \pmod{n}$ we have $p \equiv -1 \pmod{d_1}$, hence $p^{n/d} \equiv (-1)^{n/d} \equiv -1 \pmod{d_1}$, with $1 \not\equiv -1 \pmod{d_1}$. Thus for each nonunit divisor d of n we have $g = (d, p^{n/d} - 1) = 1$. Then every group $\mathbb{Z}/g\mathbb{Z}$ on which $\mathbb{Z}$ acts is trivial, so the assertion is obvious. □

The group of units of $\mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $n = 2, 4, q^k$, or $2q^k$ for $k \in \mathbb{N}$ and q an odd prime. If n is one of those values, $p^2 \equiv 1 \pmod{n}$ if and only if $p \equiv 1 \pmod{n}$ or $p \equiv -1 \pmod{n}$. So if n is one of those values, our theorems extend to the case where $p^2 \equiv 1 \pmod{n}$.

9 Ramification Groups

In this section, we introduce ramification groups, which will be useful in narrowing down the possibilities for the Galois group of the Galois closure of an extension of $\mathbb{Q}_p$.

Let $L/\mathbb{Q}_p$ be a Galois extension and let $G = Aut(L/\mathbb{Q}_p)$. We define the ith ramification group of G to be $G_i = \{\sigma \in G : \nu_L(\sigma(x) - x) \ge i + 1 \quad \forall x \in \mathcal{O}_L\}$.

Our main use of ramification groups comes from the following lemma.

Lemma 9.1. *Let $L/\mathbb{Q}_p$ be a Galois extension with ϖ a uniformizer for L and $G := \mathrm{Gal}(L/\mathbb{Q}_p)$. Let $U_i := \langle 1 + (\varpi^i)\rangle$ and let U_0 be the group of units of L. Then*

1. *For $i \ge 0$, G_i/G_{i+1} is isomorphic to a subgroup of U_i/U_{i+1} and hence is abelian.*
2. *G_0/G_1 is cyclic with order coprime to p.*
3. *G_i/G_{i+1} are direct products of cyclic groups of order p.*
4. *G_0 is the semi-direct product of a cyclic group of order coprime to p and a normal subgroup which is a p-group*
5. *G and G_0 are solvable*

Proof. See [1] pg. 43 □

For a degree 14 extension of $\mathbb{Q}_7$, the Galois group of the Galois closure must be a transitive subgroup of S_{14}. There are 63 transitive subrgoups of S_{14}. Using Lemma 9.1 we can narrow down our list of possible Galois groups even further. After doing this, we find there are 17 subgroups which satisfy these criteria.

Table 1: Possible Galois Groups for $p = 7$

Galois Group	Label (14T)	Subfields	CO	Parity	O.L. 2	O.L. 3	O.L. 4
C(14)=7[x]2	1	7T1, 2T1	14	-1			
D_14(14)=[7]2	2	7T2, 2T1	14	-1			
D(7)[x]2	3	7T2, 2T1	2	-1			
2[1/2]F_42(7)	4	7T4, 2T1	2	-1	$[7,21^2,42]$		
F_21(7)[x]2	5	7T3, 2T1	2	-1			
F_42(7)[x]2	7	7T4, 2T1	2	-1	$[7,42^2]$		
[7^2]2=7wr2	8	2T1	7	-1			
1/2[D(7)2̂]2	12	2T1	1	1	$[14^3,49]$		
[1/2.[D(7)2̂]2	13	2T1	1	-1	$[14^3,49]$	$[14^3, 28, 98^3]$	$[14^3, 28, 49^3, 98^5,$
[7^2:3]2	14	2T1	1	-1	[42,49]	$[14^2, 42, 294]$	$[14^2, 42, 98, 147, 2$
[7^2:3_3]2	15	2T1	1	-1	[42,49]	$[14^2, 42, 294]$	$[14^2, 42, 98^2, 147^3,$
[D(7)^2]2=D(7)wr2	20	2T1	1	-1	$[14^3,49]$	$[14^3, 28, 98^3]$	$[14^3, 28, 49^2, 98^6,$
[1/6_-.F_42(7)^2]2_2	22	2T1	1	1	[42,49]	[28, 42, 294]	$[28, 42, 147^3, 196,$
[1/6_+.F_42(7)^2]2_2	23	2T1	1	1	[42,49]	[28, 42, 294]	[28, 42, 147, 196, 2
[7^2:6]2	24	2T1	1	-1	[42,49]	[28, 42, 294]	[28, 42, 147, 196, 2
[7^2:6_3]2	25	2T1	1	-1	[42,49]	[28, 42, 294]	$[28, 42, 147^3, 196,$
[D(7)^2:3]2	32	2T1	1	-1	[42,49]	[28, 42, 294]	[28, 42, 147, 196, 2

Table 2: Possible Galois Groups for $p = 2$

Galois Group	Label (14T)	Subfields	Centralizer Order	Parity	Orbit Lengths 2	Orbit Lengths 3	Orbi
C(14)=7[x]2	1	7T1, 2T1	14	-1			
[2^3]7	6	7T1	2	1	$[7,28^3]$	$[14^6, 28^2, 56^4]$	
[2^4]7	9	7T1	2	-1	$[7,28^3]$	$[14^6, 56^5]$	$[7^3,$ 2
[2^6]7	21	7T1	2	1	$[7,28^3]$	$[14^6, 56^5]$	
[2^7]7=2wr7	29	7T1	2	-1	$[7,28^3]$	$[14^6, 56^5]$	$[7^3,$ 2

Table 3: Counts for Extensions of $\mathbb{Q}_7$

e	j	# $\mathcal{K}_{e,j}$	# $\mathbb{Q}_7^{e,j}$
1	0	1	1
2	0	2	2
7	1	336	27
	2	336	27
	3	336	27
	4	336	27
	5	336	27
	6	336	54
	7	343	28
14	1	84	6
	2	84	12
	3	84	6
	4	84	12
	5	84	6
	6	84	18
	8	588	48
	9	588	42
	10	588	48
	11	588	42
	12	588	96
	13	588	42
	14	686	56
			=654

Table 4: Polynomials for Unramified Extensions of $\mathbb{Q}_7$

$n = 2$	$x^2 + 6x + 3$
$n = 7$	$x^7 + 6x + 4$
$n = 14$	$x^{14} + 5x^7 + 6x^5 + 2x^4 + 3x^2 + 6x + 3$

10 Our Computations

Using Lemma 9.1 we created a program in GAP to output only the transitive subgroups of S_{14} which satisfied Lemma 9.1. The possible Galois groups for degree 14 extensions of $\mathbb{Q}_p$ must come from this list of groups. Using the T numbering system, we were able to determine that the only possible Galois Groups for degree 14 extensions of $\mathbb{Q}_7$ are of the form $14Tj$ with $j \in \{1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 15, 20, 22, 23, 24, 25, 32\}$. A similar calculation gave us that the only possible Galois Groups for degree 14 extensions of $\mathbb{Q}_2$ are of the form $14Ti$ with $i \in \{1, 6, 9, 21, 29\}$.

Then we created the p-adic field in Magma. Then, we used the AllExtensions() command in Magma, which implements an algorithm outlined by Pauli in his thesis, to get a list of all possible extensions of $\mathbb{Q}_p$ of degree 14. This algorithm gave us a list of the degree 14 irreducible polynomials defining all the extensions of $\mathbb{Q}_p$ in a given algebraic closure. Two irreducible polynomials of the same degree define isomorphic extensions if and only if one of the polynomials has a root in the field generated by the other polynomial. Using the HasRoot() command, we were able to make a list of polynomial representatives of the isomorphism classes of degree 14 extensions of $\mathbb{Q}_p$

Once we had these extensions, we began to compute properties of the field extensions and invariants of the Galois Groups in an attempt to match each field extension with its corresponding Galois Group. The group theoretic properties are listed in Tables 1 and 2.

Our first such property was subfield content. On the field theory side, for a degree 14 extension L of $\mathbb{Q}_p$, the subfield content tells us the Galois group of the Galois closures of the intermediate fields between L and $\mathbb{Q}_p$. On the LMFDB, we found polynomials defining all extensions of degree 2 and degree 7 over $\mathbb{Q}_p$. Such an extension contributes to the subfield content of L if and only if the polynomial defining the extension has a root in L. Then we used Magma's HasRoot() command to determine which polynomials had roots in which fields, thus determining subfield content. The LMFDB also contained the Galois groups of the Galois closures of these degree 2 and degree 7 subfields, so we then added these groups to our list when the corresponding polynomial had a root in the field.

On the group theory side, the subfield content is the permutation representation of the Galois Group acting on the cosets of the subgroup corresponding to the intermediate field. This information is easily calculated, but in our case, we were able to find the information in the LMFDB.

Our next invariant was the centralizer order. The centralizer order of each possible group as a subgroup of S_{14} corresponds to the size of the automorphism group of the extension. We used Magma's AutomorphismGroup() command to determine the size of the automorphism group of each extension. A program on GAP was able to determine the size of the centralizer of each possible Galois group as subgroups of S_{14}.

Then, we calculated the parity of each extension. The parity of a subgroup of S_{14} is 1 if the subgroup is contained in A_{14} and -1 otherwise. The parity of a field extension is determined by using the discriminant of the defining polynomial. The Galois Group is contained in A_{14} if and only if the discriminant of the defining polynomial is a square in $\mathbb{Q}_p$. Given a polynomial $f(x) \in \mathbb{Z}_p[x]$, factor $\mathrm{disc}(f) = p^i r$, where $r \in \mathbb{Z}_p$ and $p \nmid r$. If i is odd, the $\mathrm{disc}(f)$ is not a square. If i is even, $\mathrm{disc}(f)$ is a square if and only if $u + p\mathbb{Z}_p$ is a square in the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$.

As our tables indicate, these invariants do not give us enough information to classify the Galois group. For example, the Galois groups 14T4 and 14T7 have the same subfield content, centralizer order, and parity. To sort between these groups, we have had to use resolvent polynomials.

11 Computation of Galois Groups Using Resolvents

In most cases, the subfield content, centralizer order, and parity information are not sufficient to distinguish the Galois group of the Galois closure of a given degree 14 extension of $\mathbb{Q}_p$. In this section, we introduce a powerful tool in computational algebra for computing Galois groups, known as resolvents. As an example, we also give the explicit details of the computation a resolvent for a certain degree 14 extension of $\mathbb{Q}_7$.

Let $f(x) \in \mathbb{Q}_p[x]$ be an irreducible polynomial of degree n and set $K = \mathbb{Q}_p[x]/(f)$. Fix an algebraic closure of K and set and arbitrary ordering of the roots of f by $\alpha_1, \alpha_2, \ldots, \alpha_n$. Since f is irreducible, the Galois group of the Galois closure K^g of K is a isomoprhic to a transitive subrgoup of S_n.

Definition 1. *Let G be a subgroup of S_n containing $\mathrm{Gal}(K^g)$ and let $F(X_1, X_2, \ldots, X_m)$ be a polynomial in m variables with coeffients in $\mathbb{Z}_p$. If H is the stabilizer of F in G, that is,*

$$H = \{\sigma \in G : F(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(m)}) = F(X_1, X_2, \ldots, X_m)\},$$

we define the resolvent polynomial $R_G(F, f)$ by

$$R_G(F, f) = \prod_{\sigma \in G/H} (X - F(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})),$$

where G/H denotes any set of left coset representatives of G modulo H.

The resolvent polynomial $R_G(F, f)$ has coeffiecents in $\mathbb{Z}_p$. If $G = S_n$, we call the resolvent an absolute resolvent. Otherwise, we call the resolvent a relative resolvent. We have the following result which will be useful for computing Galois groups

Theorem 1. *Using the same notation as in the previous definition, set $l = [G : H] = \deg(R_G(F, f))$. Then if $R_G(F, f)$ is squarefree, its Galois group is equal to $\phi(\mathrm{Gal}(K^g))$, where ϕ is the natural group homomorphism from G to S_m given by the natrual left action of G on G/H. In particular, the list of the degrees of the irreducible factors of $R_G(F, f)$ in $\mathbb{Z}_p[x]$ is the same as the list of the lengths of the orbits of the action of $\phi(\mathrm{Gal}(K^g))$ on $[1, \ldots, l]$.*

It often happens that $R_G(F, f)$ is not squarefree. In that case, in order to apply the theorem we use a Tschirnhausen transformation on f to get a new irreducible polynomial defining the same extension as f. The Tschirnhausen transformation is given by the following algorithm.

Algorithm 1. *Given a monic irreducibe polynomial $f \in \mathbb{Z}_p[x]$ of degree n defining an extension of $\mathbb{Q}_p$, we find another such polynomial defining the same extension.*

1. *Choose at random a polynomial $A \in \mathbb{Z}[x]$ of degree at most $n - 1$.*
2. *Compute the resultant $U =_Y (f(Y), X - A(Y))$.*
3. *Compute $V = \gcd(U, U')$. If V is constant, then return U. Otherwise, go to step 1.*

In the case $G = S_n$ and $F = X_1 + \ldots + X_m$, then the stabillizer of F in G consists all permutations in S_n that fix $\{1, \ldots, m\} \subseteq \{1, \ldots, n\}$, and it follows that the degree of $R_{S_n}(F, f)$ is $\binom{n}{m}$. If the resolvent $R_{S_n}(F, f)$, which we shall denote from now on by $R(F, f)$ when $G = S_n$, is squarefree then the degrees of its irreducible factors correspond to the lengths of the orbits of the action of $\mathrm{Gal}(K^g)$ on the set

$$\{\{a_1, \ldots, a_m\} : a_1, \ldots, a_m \in \{1, \ldots, n\}, a_i \neq a_j \text{ if } i \neq j\}.$$

The action of $\mathrm{Gal}(K^g)$ on this set defined by the componentwise action of $\mathrm{Gal}(K^g)$ on $\{1, \ldots, n\}$. The formula for the resolvent can be written as

$$R(X_1 + \ldots + X_m, f) = \prod_{\substack{i_1 < i_2 < \ldots < i_m \\ i_1, i_2, \ldots, i_m \in \{1, \ldots, n\}}} (X - (\alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_m})).$$

We now introduce resultants as a computational tool for computing resolvents. For two polynomials $P(X), Q(X)$ over some field k we define their resultant by

$$(P, Q) = \prod_{P(x) = Q(Y) = 0} (X - Y)$$

where the roots of P and Q are in some algebraic closure of k. Note that $(P, Q) = 0$ if and only if P and Q have a common root. For our purposes, the resultant will be computed for polynomials in two variables. In this case, we will indicate by a subscript which variable should be considered the indeterminate.

Returning to the computation of resultants, when $m = 2$, we have the following formula for $R(X_1 + X_2, f)$ in terms of a resultant.

$$R(X_1 + X_2, f)(X) = \left(\frac{{}_Y(f(Y), f(X - Y))}{2^n f(X/2)} \right)^{1/2}.$$

Table ?? shows the lengths of the orbits of the possible Galois groups of a degree 14 extension of $\mathbb{Q}_7$ acting on subsets of $1, \ldots,$ of size 2. From this table, it is clear that we may distiniguish between the groups $14T4$ and $14T7$ by using the degree 91 resolvent $R(X_1 + X_2, f)(X)$. The following section gives an example computation of such a resolvent.

11.1 Example computation of a resolvent

In this brief section we give the details of the computation of a degree 91 resolvent which allows us to distinguish between the Galois groups 14T4 and 14T7. We start with the irreducible polynomial $f(x) = x^{14} + 63x^8 + 42x^4 + 7 \in \mathbb{Z}_7[x]$. The extension of $\mathbb{Q}_7$ defined by f has subfields 2T1 and 7T4, and centralizer order 2. From table ??, it follows that we can look at the degrees of the irreducible factors of $R(X_1 + X_2, f)(X)$ to determine the Galois group of f.

Using the computer algebra system MAGMA, we compute this resolvent using the resultant formula from the previous section. Since the computation of such resultants in MAGMA using 7-adic numbers is slow, we perform the resultant computation using polynomials with coefficients in $\mathbb{Q}$. The polynomial division operations are also performed using polynomials with rational coefficients. After completing these operations, we are left with the degree 182 polynomial $(R(X_1 + X_2, f)(X))^2$, the square of our desired resultant. This polynomial has integer cefficients, and we do not write the polynomial here due to its large size. There is no easy way to take the square root of such a polynomial, but we do not have to in this case becuase it is immediately clear by inspection that the resolvent will have a factor of x^7, and hence it will not be squarefree.

It is necessary to apply a Tschirnhausen transformation to f. The random polynomial for the Tschirnhausen transformation is computed having integer coefficients between -100 and 100. The resultant operation in Algorithm ?? is again performed using polynomials over the rationals to save time. This resultant is guaranteed to have integer coefficients. The GCD in step 3 is computed using polynomials defined over $\mathbb{Z}_7$. In our case, the Tschirnhausen transformation gave us the irreducible polynomial

$$\begin{aligned}\tilde{f} = x^{14} &- 159386430x^{13} + 10634011442862563x^{12} \\ &- 37945365917340090911319 8x^{11} + 9568189246566286288325 24x^{10} \\ &- 743023554170267867907 41x^{9} + 66701289893264609446863 02x^{8} \\ &- 84162555129996599487329 90x^{7} - 51905905979030575170405 14x^{6} \\ &+ 57541757224778840191904 32x^{5} + 69661462697133835344655 37x^{4} \\ &- 10832766079412731838804 252x^{3} - 65597742132953331392723 94x^{2} \\ &- 95800025661705705654481 65x + 70383000253238214406690 79.\end{aligned}$$

We now compute the square of the resolvent $R(X_1 + X_2, \tilde{f})(X)$ as before. Factoring this degree 182 polynomial over $\mathbb{Q}_7$ and removing one copy of each factor to get the square root, we are left with the factorization of the resolvent $R(X_1 + X_2, \tilde{f})(X)$ over $\mathbb{Q}_7$. In our case, this polynomial turned out to be squarefree and had irreducible factors of degrees 7, 21, 21 and 42. We can then conclude that the Galois group of f is 14T4.

12 Degree 14 Extensions of $\mathbb{Q}_7$

The following table gives a list of defining polynomials for all degree 14 Extensions of $\mathbb{Q}_7$. The e column is the ramification index of the extension, the j column is the j from Ore's condition. The sgg content column is the subfield content of the extension, the C.O. column is the size of the automorphism group and the parity is 1 if the discriminant of the polynomial is a square in $\mathbb{Q}_7$. The G column is the Galois group of the extension.

Table 5: Extensions of $\mathbb{Q}_7$

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}-84x^{12}+49x^{10}-42x^7+49x^5+105$	14	5	2T1	1	-1	
$x^{14}+7x^{12}+21$	14	5	2T1, 7T3	2	1	
$x^{14}-91x^{12}+98x^{10}-91x^7-147x^5-28$	14	5	2T1	1	-1	
$x^{14}-91x^{12}+98x^{10}+161x^7+49x^5-77$	14	5	2T1	1	1	
$x^{14}-91x^{12}+98x^{10}+70x^7-98x^5+70$	14	5	2T1	1	-1	
$x^{14}+7x^{12}+35$	14	5	2T1, 7T3	2	1	
$x^{14}+161x^{12}+49x^{10}-91x^7+49x^5-28$	14	5	2T1	1	-1	
$x^{14}+161x^{12}+49x^{10}+161x^7+98x^5-77$	14	5	2T1	1	1	
$x^{14}+161x^{12}+49x^{10}+70x^7+147x^5+70$	14	5	2T1	1	-1	
$x^{14}+21x^{12}+21$	14	5	2T1, 7T2	2	1	
$x^{14}+70x^{12}-147x^{10}-91x^7-98x^5-28$	14	5	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} + 70x^{12} - 147x^{10} + 161x^7 + 147x^5 - 77$	14	5	2T1	1	1	
$x^{14} + 70x^{12} - 147x^{10} + 70x^7 + 49x^5 + 70$	14	5	2T1	1	-1	
$x^{14} - 21x^{12} - 147x^{10} - 126$	14	5	2T1, 7T1	14	1	
$x^{14} + 14x^{12} + 35$	14	5	2T1, 7T1	14	-1	
$x^{14} - 21x^{12} - 147x^{10} + 168$	14	5	2T1, 7T1	14	1	
$x^{14} - 21x^{12} - 147x^{10} - 28$	14	5	2T1, 7T1	14	-1	
$x^{14} + 14x^{12} + 84$	14	5	2T1, 7T1	14	1	
$x^{14} + 7x^{12} + 91$	14	5	2T1, 7T1	14	-1	
$x^{14} + 7x^{12} + 42$	14	5	2T1, 7T1	14	1	
$x^{14} - 21x^{12} - 147x^{10} - 91x^7 + 98x^5 - 28$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} - 91x^7 + 98x^5 + 119$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} - 91x^7 + 98x^5 - 77$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} - 91x^7 + 98x^5 + 70$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} - 91x^7 + 98x^5 - 126$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} - 91x^7 + 98x^5 + 21$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} - 91x^7 + 98x^5 + 168$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} + 161x^7 - 147x^5 - 77$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} + 161x^7 - 147x^5 + 70$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} + 161x^7 - 147x^5 - 126$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} + 161x^7 - 147x^5 + 21$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} + 161x^7 - 147x^5 + 168$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} + 161x^7 - 147x^5 - 28$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} + 161x^7 - 147x^5 + 119$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 + 70$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 - 126$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 + 21$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 + 168$	14	5	2T1	7	1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 - 28$	14	5	2T1	7	-1	
$x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 + 119$	14	5	2T1	7	1	
$x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 - 77$	14	5	2T1	7	-1	
$x^{14} + 21x^{12} + 42$	14	5	2T1, 7T4	2	1	
$x^{14} - 112x^{12} + 49x^{10} - 91x^7 - 49x^5 - 28$	14	5	2T1	1	-1	
$x^{14} - 112x^{12} + 49x^{10} + 161x^7 - 98x^5 - 77$	14	5	2T1	1	1	
$x^{14} - 112x^{12} + 49x^{10} + 70x^7 - 147x^5 + 70$	14	5	2T1	1	-1	
$x^{14} + 21x^{12} + 35$	14	5	2T1, 7T4	2	1	
$x^{14} + 140x^{12} + 98x^{10} - 91x^7 + 147x^5 - 28$	14	5	2T1	1	-1	
$x^{14} + 140x^{12} + 98x^{10} + 161x^7 - 49x^5 - 77$	14	5	2T1	1	1	
$x^{14} + 140x^{12} + 98x^{10} + 70x^7 + 98x^5 + 70$	14	5	2T1	1	-1	
$x^{14} + 7x + 22$	7	-6	2T1	1	1	
$x^{14} + 7x + 11$	7	-6	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 42x^8 - 141x^7 + 161x^6 - 77x^5 - 98x^4 + 91x^3 + 112x^2 - 49x - 95$	7	-6	2T1	1	1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 41x^7 + 63x^6 - 77x^5 + 140x^3 - 84x^2 - 161x - 102$	7	-6	2T1	1	-1	
$x^{14} + 7x + 18$	7	-6	2T1	1	1	
$x^{14} + 7x + 8$	7	-6	2T1	1	-1	
$x^{14} + 49x + 2$	7	-6	2T1, 7T4	2	-1	
$x^{14} + 7x + 32$	7	-6	2T1	1	-1	
$x^{14} + y^7 + 32$	7	-6	2T1	1	-1	
$x^{14} + 7x + 1$	7	-6	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 14x^8 + 34x^7 - 35x^6 + 70x^5 + 98x^4 + 91x^3 - 35x^2 - 168x + 59$	7	-6	2T1	1	-1	
$x^{14} + 98x + 98$	7	-6	2T1	1	-1	
$x^{14} + 7x^2 + 1$	7	-6	2T1, 7T4	2	-1	
$x^{14} + 7x + 9$	7	-6	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 112x^8 + 6x^7 + 63x^6 - 126x^5 - 56x^3 - 84x^2 - 147x + 136$	7	-6	2T1	1	1	
$x^{14} + 7x + 23$	7	-6	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+28x^8+27x^7-133x^6-126x^5-147x^4+42x^3+112x^2+70x+171$	7	-6	2T1	1	-1	
$x^{14}+7x+16$	7	-6	2T1, 7T4	2	-1	
$x^{14}+49x+98$	7	-6	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+126x^8-y^7-35x^6+21x^5+98x^4-105x^3+63x^2+91x-95$	7	-6	2T1	1	-1	
$x^{14}+7x+36$	7	-6	2T1	1	1	
$x^{14}+7x+37$	7	-6	2T1, 7T4	2	-1	
$x^{14}+7x+2$	7	-6	2T1	1	-1	
$x^{14}+y^7+4$	7	-6	2T1	1	-1	
$x^{14}+28x^2+1$	7	-6	2T1, 7T4	2	-1	
$x^{14}+7x+4$	7	-6	2T1	1	-1	
$x^{14}+35x^2+1$	7	-6	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}-7x^9+140x^8-57x^7-84x^6+119x^5-56x^3-98x^2+77x-25$	7	-5	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}-49x^9+112x^8-113x^7+63x^6-28x^5+42x^3+84x^2-133x+122$	7	-5	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}-91x^9+84x^8-169x^7-133x^6+168x^5-49x^4-105x^3-77x^2-49x+171$	7	-5	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}-133x^9+56x^8+118x^7+14x^6+21x^5-147x^4-154x^3+105x^2-14x+122$	7	-5	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+168x^9+28x^8+62x^7+161x^6-126x^5+49x^4-105x^3-56x^2-28x-25$	7	-5	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+126x^9+6x^7-35x^6+70x^5-147x^4+42x^3+126x^2-91x+73$	7	-5	2T1	1	1	
$x^{14}+42x^2+8$	7	-5	2T1, 7T3	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+7x^9-168x^8+6x^7+161x^6-126x^5-49x^4-154x^3-7x^2+56x-165$	7	-5	2T1	1	1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} - 35x^9 + 147x^8 - 50x^7 - 35x^6 + 70x^5 - 154x^3 - 168x^2 - 105x + 80$	7	-5	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} - 77x^9 + 119x^8 - 106x^7 + 112x^6 - 77x^5 - 56x^3 + 14x^2 + 28x - 116$	7	-5	2T1	1	1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} - 119x^9 + 91x^8 - 162x^7 - 84x^6 + 119x^5 - 49x^4 + 140x^3 - 147x^2 + 112x - 67$	7	-5	2T1	1	-1	
$x^{14} + 7x^9 + 98$	7	-5	2T1	1	-1	
$x^{14} + 42x^2 + 4$	7	-5	2T1, 7T3	2	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 21x^9 - 133x^8 + 69x^7 + 63x^6 - 28x^5 - 105x^3 + 84x^2 + 133x - 109$	7	-5	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} - 21x^9 - 161x^8 + 13x^7 - 133x^6 + 168x^5 + 98x^4 + 140x^3 - 77x^2 + 21x - 109$	7	-5	2T1	1	-1	
$x^{14} + 7x^9 + 49$	7	-5	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} - 105x^9 + 126x^8 - 99x^7 + 161x^6 - 126x^5 + 147x^4 - 105x^3 - 56x^2 - 7x - 60$	7	-5	2T1	1	-1	
$x^{14} + 42x^2 + 2$	7	-5	2T1, 7T4	2	-1	
$x^{14} + 14x^9 + 49$	7	-5	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} - 7x^9 - 126x^8 + 76x^7 + 112x^6 - 77x^5 - 49x^4 - 105x^3 + 14x^2 - 98x - 102$	7	-5	2T1	1	1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} - 49x^9 - 154x^8 + 20x^7 - 84x^6 + 119x^5 + 49x^4 + 140x^3 - 147x^2 + 133x - 102$	7	-5	2T1	1	-1	
$x^{14} + 42x^2 + 1$	7	-5	2T1, 7T3	2	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 49x^9 - 63x^8 - 148x^7 - 133x^6 + 168x^5 + 49x^4 + 91x^3 - 77x^2 - 105x - 95$	7	-5	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 7x^9 - 91x^8 + 139x^7 + 14x^6 + 21x^5 - 98x^4 + 140x^3 + 105x^2 - 119x + 101$	7	-5	2T1	1	-1	
$x^{14} + 42x^2 + 9$	7	-5	2T1, 7T4	2	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+63x^9-28x^8-85x^7+112x^6-77x^5+49x^4-105x^3+14x^2-77x-137$	7	-5	2T1	1	1	
$x^{14}+42x^2+29$	7	-5	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-91x^{10}+140x^9+49x^8-y^7+14x^6+168x^5-49x^4+77x^3-105x^2-154x-4$	7	-4	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-133x^{10}-98x^9-70x^8-y^7-133x^6-126x^5+49x^4+112x^3+21x^2+91x-32$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}+168x^{10}+7x^9+154x^8-y^7+14x^6+70x^5-98x^4+49x^3+98x^2-56x-11$	7	-4	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}+126x^{10}+112x^9+35x^8-y^7+112x^6+70x^5-147x^4-112x^3+126x^2+91x+59$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}+84x^{10}-126x^9-84x^8-y^7+161x^6-126x^5-98x^4-28x^3+105x^2-154x-165$	7	-4	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}+42x^{10}-21x^9+140x^8-y^7+161x^6+168x^5+49x^4-42x^3+35x^2-105x+3$	7	-4	2T1	1	-1	
$x^{14}+7x^{10}+98$	7	-4	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-77x^{10}-126x^9+140x^8-43x^7+63x^6-126x^5-49x^4+70x^3+35x^2-84x-53$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-119x^{10}-21x^9+21x^8-43x^7-35x^6+119x^5-49x^4-140x^3-133x^2-133x-130$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-161x^{10}+84x^9-98x^8-43x^7+161x^6+168x^5+49x^4-105x^3-7x^2+112x-158$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}+140x^{10}-154x^9+126x^8-43x^7-35x^6+21x^5-98x^4-168x^3+70x^2-35x-137$	7	-4	2T1	1	-1	
$x^{14}+49x^3+98$	7	-4	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+14x^{10}+98$	7	-4	2T1, 7T2	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-63x^{10}-49x^9-112x^8-85x^7-133x^6-28x^5+98x^4-84x^3-70x^2+84x+143$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-105x^{10}+56x^9+112x^8-85x^7+161x^6+70x^5+147x^3+154x^2+84x+17$	7	-4	2T1	1	1	
$x^{14}+49x^3+49$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}+154x^{10}-77x^9-126x^8-85x^7-84x^6+21x^5+98x^4-28x^3+112x^2-63x-88$	7	-4	2T1	1	-1	
$x^{14}+21x^{10}+98$	7	-4	2T1, 7T4	2	-1	
$x^{14}+98x^3+49$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-91x^{10}+133x^9-140x^8-127x^7+112x^6+70x^5-147x^4-56x^3-147x^2+56x+66$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-133x^{10}-105x^9+84x^8-127x^7+63x^6+168x^5+98x^4-168x^3+77x^2+56x-60$	7	-4	2T1	1	1	
$x^{14}+7x^{10}+49$	7	-4	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-35x^{10}+105x^9+70x^8-169x^7+112x^6-28x^5+147x^4-147x^3+14x^2+28x-102$	7	-4	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-77x^{10}-133x^9-49x^8-169x^7+161x^6+119x^5-147x^4-63x^3-7x^2+126x+17$	7	-4	2T1	1	-1	
$x^{14}+21x^{10}+49$	7	-4	2T1, 7T2	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-21x^{10}-161x^9+161x^8+132x^7-133x^6-126x^5+49x^4-56x^3-140x^2+147x+143$	7	-4	2T1	1	-1	
$x^{14}+35x^{10}+49$	7	-4	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+42x^{11}-154x^{10}+91x^9-126x^8+69x^7+112x^6+168x^5+84x^4-35x^3-35x^2-21x-144$	7	-3	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{10}+147x^9-126x^8-8x^7-84x^6-28x^5-126x^4+35x^3+161x^2-133x+129$	7	-3	2T1	1	1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+42x^{13}+91x^{12}-42x^{11}-21x^{10}-140x^9+168x^8+111x^7-133x^6+21x^5+7x^4+154x^3-35x^2-98x-137$	7	-3	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}-84x^{11}-126x^{10}-84x^9+70x^8+83x^7-35x^6-28x^5+140x^4-21x^3+63x^2+84x+87$	7	-3	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}-126x^{11}+112x^{10}-28x^9-77x^8-92x^7-133x^6+168x^5-70x^4-147x^3+112x^2+70x+115$	7	-3	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}-168x^{11}+7x^{10}+28x^9+70x^8-71x^7-84x^6-77x^5+63x^4+119x^3+112x^2-140x-53$	7	-3	2T1	1	1	
$x^{14}+49x^4+98$	7	-3	2T1, 7T3	2	-1	
$x^{14}+42x^{13}+91x^{12}+56x^{11}-35x^{10}+77x^9+49x^8-29x^7+63x^6-126x^5-70x^4+70x^3+7x^2-70x-165$	7	-3	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}+14x^{11}-140x^{10}+133x^9+98x^8+41x^7+63x^6+119x^5+63x^4+91x^3-91x^2+14x-39$	7	-3	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}-28x^{11}+98x^{10}-154x^9+98x^8-36x^7-133x^6-77x^5-147x^4+161x^3+105x^2-98x-109$	7	-3	2T1	1	1	
$x^{14}+42x^{13}+91x^{12}-70x^{11}-7x^{10}-98x^9+49x^8+83x^7+161x^6-28x^5-14x^4-63x^3-91x^2-63x-32$	7	-3	2T1	1	-1	
$x^{14}+21x^{11}+49$	7	-3	2T1	1	-1	
$x^{14}+98x^4+98$	7	-3	2T1, 7T3	2	-1	
$x^{14}+42x^{13}+91x^{12}+70x^{11}+84x^{10}+63x^9-21x^8+167x^7+63x^6+119x^5+119x^4+77x^3+147x^2-70x-137$	7	-3	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+28x^{11}-21x^{10}+119x^9+77x^8+41x^7-84x^6+119x^5-91x^4+49x^3+98x^2-133x-158$	7	-3	2T1	1	-1	
$x^{14}+7x^{11}+49$	7	-3	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} + 42x^{13} + 91x^{12} - 56x^{11} + 112x^{10} - 112x^9 + 126x^8 + 34x^7 + 63x^6 + 168x^5 - 168x^4 + 140x^3 - 147x^2 - 161x - 102$	7	-3	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 126x^{11} - 35x^{10} - 7x^9 + 154x^8 + 146x^7 - 133x^6 + 21x^5 - 168x^4 + 112x^3 - 7x^2 - 7x - 88$	7	-3	2T1, 7T4	2	-1	
$x^{14} + 14x^{11} + 49$	7	-3	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 42x^{11} + 98x^{10} + 105x^9 + 154x^8 - 8x^7 + 161x^6 - 28x^5 + 98x^4 - 91x^3 + 42x^2 + 112x + 115$	7	-3	2T1	1	1	
$x^{14} + 42x^{13} + 91x^{12} - 7x^{10} + 161x^9 - 91x^8 - 134x^7 + 14x^6 - 28x^5 - 112x^4 - 119x^3 - 7x^2 + 49x + 94$	7	-3	2T1	1	-1	
$x^{14} + 49x^4 + 49$	7	-3	2T1, 7T3	2	-1	
$x^{14} + 42x^{13} + 91x^{12} + 98x^{11} - 21x^{10} + 35x^9 + 133x^8 + 69x^7 - 133x^6 + 168x^5 + 154x^4 + 140x^3 + 35x^2 + 77x + 66$	7	-3	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 56x^{11} - 126x^{10} + 91x^9 - 14x^8 - 106x^7 + 112x^6 + 21x^5 - 56x^4 + 14x^3 + 84x^2 + 63x + 94$	7	-3	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 154x^{11} - 140x^{10} - 35x^9 + 63x^8 - y^7 + 63x^6 - 77x^5 - 133x^4 + 77x^3 - 21x^2 - 154x + 164$	7	-3	2T1, 7T4	2	-1	
$x^{14} + 42x^{13} + 91x^{12} + 112x^{11} + 98x^{10} + 21x^9 + 14x^8 + 118x^7 + 14x^6 - 28x^5 - 147x^3 + 126x^2 - 119x - 102$	7	-3	2T1	1	1	
$x^{14} + 42x^{13} + 91x^{12} + 168x^{11} - 21x^{10} - 49x^9 - 7x^8 - 148x^7 + 63x^6 + 168x^5 + 56x^4 + 84x^3 + 119x^2 - 154x - 151$	7	-3	2T1, 7T4	2	-1	
$x^{14} + 42x^{13} + 49x^{12} + 112x^{11} - 119x^{10} - 161x^9 + 28x^8 + 125x^7 + 112x^6 + 56x^5 + 63x^4 - 56x^3 + 77x^2 + 35x - 116$	7	-2	2T1	1	1	
$x^{14} + 42x^{13} + 7x^{12} + 140x^{11} + 105x^{10} - 112x^9 + 35x^8 - 92x^7 - 35x^6 - 56x^5 + 77x^4 - 56x^3 - 56x^2 + 126x + 136$	7	-2	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+42x^{13}-35x^{12}+168x^{11}-63x^{10}-161x^9-154x^8+34x^7+14x^6-70x^5-7x^4-56x^3+7x^2+168x+143$	7	-2	2T1	1	1	
$x^{14}+42x^{13}-77x^{12}-147x^{11}+63x^{10}+35x^9+147x^8+160x^7-84x^6+14x^5+154x^4-56x^3-77x^2+161x-95$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}-119x^{12}-119x^{11}+140x^{10}+133x^9-91x^8-57x^7+14x^6-147x^5-126x^4-56x^3+35x^2+105x+108$	7	-2	2T1	1	1	
$x^{14}+42x^{13}-161x^{12}-91x^{11}+168x^{10}+133x^9+161x^8+69x^7-35x^6+133x^5-161x^4-56x^3+66$	7	-2	2T1	1	-1	
$x^{14}+21x^{12}+98$	7	-2	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+63x^{12}-70x^{11}+70x^{10}+56x^9+126x^8+55x^7+161x^6+98x^5-14x^4+63x^3-168x^2-119x+150$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}+21x^{12}-42x^{11}-140x^9-14x^8-162x^7+161x^6-112x^5+98x^4+63x^3-154x^2+21x-39$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}-21x^{12}-14x^{11}-119x^{10}-91x^9-7x^8-36x^7+14x^6+119x^5+112x^4+63x^3+56x^2+112x-130$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}-63x^{12}+14x^{11}+56x^{10}-140x^9+147x^8+90x^7+63x^6+105x^5+28x^4+63x^3+119x^2+154x-123$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}-105x^{12}+42x^{11}-161x^{10}+56x^9+105x^8-127x^7-35x^6-154x^5-154x^4+63x^3+35x^2+147x-18$	7	-2	2T1	1	-1	
$x^{14}+21x^{12}+49$	7	-2	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+77x^{12}+91x^{11}+14x^{10}+126x^9-70x^8-15x^7+161x^6-56x^5+105x^4-161x^3-119x^2+168x-123$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}+35x^{12}+119x^{11}-7x^{10}+28x^9-14x^8+111x^7-35x^6-21x^5-28x^4-161x^3+42x^2+14x-67$	7	-2	2T1	1	1	
$x^{14}+49x^5+49$	7	-2	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+42x^{13}-49x^{12}-168x^{11}+147x^{10}-119x^9-147x^8+20x^7+161x^6+98x^4-161x^3-77x^2-98x-4$	7	-2	2T1	1	-1	
$x^{14}+7x^{12}+49$	7	-2	2T1, 7T4	2	-1	
$x^{14}+98x^5+49$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}+49x^{12}-63x^{11}+84x^{10}+49x^9+35x^8+41x^7+63x^6-126x^5+42x^4-42x^3-154x^2+105x+52$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}+7x^{12}-35x^{11}+63x^{10}-49x^9+91x^8+167x^7-133x^6-91x^5-91x^4-42x^3+7x^2-49x+108$	7	-2	2T1	1	1	
$x^{14}+35x^{12}+98$	7	-2	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+105x^{12}+70x^{11}-147x^{10}+168x^9+28x^8-155x^7+14x^6+77x^5-98x^4+77x^3-168x^2+7x+115$	7	-2	2T1	1	-1	
$x^{14}+42x^{13}+63x^{12}+98x^{11}-70x^{10}-77x^9+133x^8-29x^7+112x^6-84x^5-35x^4+77x^3-56x^2-49x-25$	7	-2	2T1	1	-1	
$x^{14}+7x^{12}+98$	7	-2	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+119x^{12}-112x^{11}+91x^{10}+140x^9-21x^8+118x^7-133x^6+21x^5-77x^4-147x^3+77x^2-98x-60$	7	-2	2T1	1	-1	
$x^{14}+14x^{12}+49$	7	-2	2T1, 7T4	2	-1	
$x^{14}+56x^{12}-21x^{11}-147x^{10}+154x^9-7x^8+55x^7+98x^6+126x^5+49x^4-77x^3-154x^2-63x-165$	7	-1	2T1	1	-1	
$x^{14}-42x^{13}-28x^{12}+168x^{11}-147x^{10}-168x^9+112x^8+13x^7+133x^6+35x^5+49x^4+21x^2+77x-109$	7	-1	2T1	1	1	
$x^{14}-84x^{13}-161x^{12}-35x^{11}-49x^{10}+98x^9-161x^8-127x^7-126x^6-7x^5-49x^4-168x^3-98x^2-28x-102$	7	-1	2T1	1	-1	
$x^{14}-126x^{13}+56x^{11}+147x^{10}-77x^9-140x^8-22x^7+7x^6+98x^4+105x^3-168x^2-35x-144$	7	-1	2T1	1	1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}-168x^{13}+112x^{12}+98x^{11}+98x^{10}-7x^9-168x^8-15x^7-154x^6+56x^5+147x^4+133x^3+154x^2+56x+108$	7	-1	2T1	1	-1	
$x^{14}+133x^{13}-168x^{12}+91x^{11}+147x^{10}-35x^9+98x^8-106x^7+77x^6+161x^5+98x^4-84x^3-161x^2-98x-32$	7	-1	2T1	1	1	
$x^{14}+56x^{13}-147x^{11}+91x^{10}-14x^9-154x^8+69x^7+56x^6-140x^5+7x^4-7x^3-154x^2-77x+17$	7	-1	2T1, 7T2	14	-1	
$x^{14}+56x^{13}-147x^{11}+91x^{10}-14x^9-154x^8+118x^7+56x^6-140x^5+7x^4-7x^3-154x^2-77x-81$	7	-1	2T1	7	-1	
$x^{14}+56x^{13}-147x^{11}+91x^{10}-14x^9-154x^8+167x^7+56x^6-140x^5+7x^4-7x^3-154x^2-77x+164$	7	-1	2T1	7	-1	
$x^{14}+56x^{13}-147x^{11}+91x^{10}-14x^9-154x^8-127x^7+56x^6-140x^5+7x^4-7x^3-154x^2-77x+66$	7	-1	2T1	7	-1	
$x^{14}+14x^{13}+14x^{12}+140x^{11}-105x^{10}-140x^9+63x^8-120x^7-7x^6+14x^5-140x^4-126x^3-77x^2-133x+171$	7	-1	2T1	1	-1	
$x^{14}-28x^{13}-21x^{12}+35x^{11}+140x^{10}-21x^9-112x^8-64x^7-21x^6-126x^5-42x^4-147x^3+49x^2-91x-67$	7	-1	2T1	7	-1	
$x^{14}-28x^{13}-21x^{12}+35x^{11}+140x^{10}-21x^9-112x^8-15x^7-21x^6-126x^5-42x^4-147x^3+49x^2-91x-165$	7	-1	2T1	7	-1	
$x^{14}-28x^{13}-21x^{12}+35x^{11}+140x^{10}-21x^9-112x^8+34x^7-21x^6-126x^5-42x^4-147x^3+49x^2-91x+80$	7	-1	2T1	7	-1	
$x^{14}-28x^{13}-21x^{12}+35x^{11}+140x^{10}-21x^9-112x^8+83x^7-21x^6-126x^5-42x^4-147x^3+49x^2-91x-18$	7	-1	2T1	7	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} - 28x^{13} - 21x^{12} + 35x^{11} + 140x^{10} - 21x^9 - 112x^8 + 132x^7 - 21x^6 - 126x^5 - 42x^4 - 147x^3 + 49x^2 - 91x - 116$	7	-1	2T1	7	-1	
$x^{14} - 28x^{13} - 21x^{12} + 35x^{11} + 140x^{10} - 21x^9 - 112x^8 - 162x^7 - 21x^6 - 126x^5 - 42x^4 - 147x^3 + 49x^2 - 91x + 129$	7	-1	2T1	7	-1	
$x^{14} - 28x^{13} - 21x^{12} + 35x^{11} + 140x^{10} - 21x^9 - 112x^8 - 113x^7 - 21x^6 - 126x^5 - 42x^4 - 147x^3 + 49x^2 - 91x + 31$	7	-1	2T1	7	-1	
$x^{14} - 70x^{13} - 105x^{12} - 119x^{11} + 140x^{10} + 7x^8 - 106x^7 + 14x^6 + 126x^5 - 42x^4 - 70x^3 - 119x^2 + 49x - 11$	7	-1	2T1	1	-1	
$x^{14} - 112x^{13} + 105x^{12} + 21x^{11} - 105x^{10} - 77x^9 + 77x^8 + 97x^7 + 98x^6 + 84x^5 - 140x^4 + 105x^3 + 105x^2 - 56x - 4$	7	-1	2T1	1	-1	
$x^{14} + 14x^{13} + 98$	7	-1	2T1	1	-1	
$x^{14} + 70x^{13} + 7x^{12} + 63x^{11} + 35x^{10} + 133x^9 - 35x^8 - 8x^7 - 98x^6 + 42x^5 - 84x^4 - 154x^3 - 126x^2 + 98x + 59$	7	-1	2T1, 7T4	2	-1	
$x^{14} + 28x^{13} + 70x^{12} + 56x^{11} + 84x^{10} + 105x^9 - 112x^8 - 99x^7 + 133x^6 + 147x^5 - 133x^4 - 28x^3 - 98x^2 - 56x - 81$	7	-1	2T1	1	-1	
$x^{14} - 14x^{13} + 84x^{12} - 112x^{10} - 21x^9 + 105x^8 + 55x^7 + 70x^6 - 42x^5 + 63x^4 - 147x^3 - 21x^2 - 112x + 73$	7	-1	2T1	1	1	
$x^{14} + 7x^{13} + 49$	7	-1	2T1	1	-1	
$x^{14} - 98x^{13} - 35x^{12} + 84x^{11} + 133x^{10} + 119x^9 + 49x^8 + 69x^7 + 91x^6 + 70x^5 + 161x^4 - 91x^3 - 63x^2 + 70x - 109$	7	-1	2T1	1	-1	
$x^{14} + 49x^6 + 49$	7	-1	2T1, 7T3	2	-1	
$x^{14} + 14x^{13} + 49$	7	-1	2T1	7	-1	
$x^{14} + 42x^{13} - 119x^{12} + 70x^{11} + 77x^{10} - 140x^9 + 154x^8 + 167x^7 - 168x^6 - 161x^5 + 70x^4 - 126x^3 + 126x^2 + 168x + 10$	7	-1	2T1	7	-1	
$x^{14} + 7x^{13} + 98$	7	-1	2T1	7	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} + 42x^{13} - 119x^{12} + 70x^{11} + 77x^{10} - 140x^9 + 154x^8 - 78x^7 - 168x^6 - 161x^5 + 70x^4 - 126x^3 + 126x^2 + 168x + 157$	7	-1	2T1	7	-1	
$x^{14} + 42x^{13} - 119x^{12} + 70x^{11} + 77x^{10} - 140x^9 + 154x^8 - 29x^7 - 168x^6 - 161x^5 + 70x^4 - 126x^3 + 126x^2 + 168x + 59$	7	-1	2T1	7	-1	
$x^{14} + 42x^{13} - 119x^{12} + 70x^{11} + 77x^{10} - 140x^9 + 154x^8 + 20x^7 - 168x^6 - 161x^5 + 70x^4 - 126x^3 + 126x^2 + 168x - 39$	7	-1	2T1	7	-1	
$x^{14} + 42x^{13} - 119x^{12} + 70x^{11} + 77x^{10} - 140x^9 + 154x^8 + 69x^7 - 168x^6 - 161x^5 + 70x^4 - 126x^3 + 126x^2 + 168x - 137$	7	-1	2T1	7	-1	
$x^{14} - 56x^{12} + 63x^{11} + 126x^{10} - 168x^9 + 77x^8 + 27x^7 + 63x^6 - 56x^5 + 21x^4 + 154x^2 + 14x - 32$	7	-1	2T1	1	-1	
$x^{14} - 42x^{13} - 42x^{12} + 7x^{11} - 70x^{10} + 49x^9 - 49x^8 - 162x^7 + 98x^5 - 126x^4 - 119x^3 - 112x^2 - 42x + 122$	7	-1	2T1	1	1	
$x^{14} + 98x^{13} - 28x^{12} + 91x^{11} + 21x^{10} - 14x^9 + 154x^8 + 83x^7 - 14x^6 + 112x^5 - 21x^4 - 7x^3 - 21x^2 - 140x + 94$	7	-1	2T1, 7T4	2	-1	
$x^{14} + 56x^{13} + 133x^{12} - 161x^{11} - 126x^{10} + 154x^9 - 168x^8 - 155x^7 + 119x^6 + 119x^5 + 126x^4 - 77x^3 - 91x^2 - 147x + 52$	7	-1	2T1	1	-1	
$x^{14} + 14x^{13} - 98x^{12} - 119x^{11} + 168x^{10} - 119x^9 + 147x^8 - 148x^7 - 42x^6 - 168x^5 - 168x^4 - 49x^3 - 112x^2 - 56x - 39$	7	-1	2T1	7	-1	
$x^{14} + 14x^{13} - 98x^{12} - 119x^{11} + 168x^{10} - 119x^9 + 147x^8 - 99x^7 - 42x^6 - 168x^5 - 168x^4 - 49x^3 - 112x^2 - 56x - 137$	7	-1	2T1	7	-1	
$x^{14} + 14x^{13} - 98x^{12} - 119x^{11} + 168x^{10} - 119x^9 + 147x^8 - 50x^7 - 42x^6 - 168x^5 - 168x^4 - 49x^3 - 112x^2 - 56x + 108$	7	-1	2T1	7	-1	
$x^{14} + 14x^{13} - 98x^{12} - 119x^{11} + 168x^{10} - 119x^9 + 147x^8 - y^7 - 42x^6 - 168x^5 - 168x^4 - 49x^3 - 112x^2 - 56x + 10$	7	-1	2T1	7	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+14x^{13}-98x^{12}-119x^{11}+168x^{10}-119x^9+147x^8+48x^7-42x^6-168x^5-168x^4-49x^3-112x^2-56x-88$	7	-1	2T1	7	-1	
$x^{14}+14x^{13}-98x^{12}-119x^{11}+168x^{10}-119x^9+147x^8+97x^7-42x^6-168x^5-168x^4-49x^3-112x^2-56x+157$	7	-1	2T1	7	-1	
$x^{14}+14x^{13}-98x^{12}-119x^{11}+168x^{10}-119x^9+147x^8+146x^7-42x^6-168x^5-168x^4-49x^3-112x^2-56x+59$	7	-1	2T1	7	-1	
$x^{14}+49x^6+98$	7	-1	2T1, 7T3	2	-1	
$x^{14}+70x^{13}+140x^{12}+49x^{11}+161x^{10}-42x^9-49x^8+111x^7-35x^6-42x^5+35x^4+119x^3-63x^2+28x+94$	7	-1	2T1	1	-1	
$x^{14}+98x^6+49$	7	-1	2T1, 7T1	14	-1	
$x^{14}+126x^{13}-14x^{12}+168x^{11}-91x^{10}-63x^9+49x^8-22x^7+21x^6+133x^5+140x^4+42x^3+35x^2-133x+80$	7	-1	2T1, 7T1	14	-1	
$x^{14}+126x^{13}-14x^{12}+168x^{11}-91x^{10}-63x^9+49x^8+27x^7+21x^6+133x^5+140x^4+42x^3+35x^2-133x-18$	7	-1	2T1, 7T1	14	-1	
$x^{14}+126x^{13}-14x^{12}+168x^{11}-91x^{10}-63x^9+49x^8+76x^7+21x^6+133x^5+140x^4+42x^3+35x^2-133x-116$	7	-1	2T1, 7T1	14	-1	
$x^{14}+126x^{13}-14x^{12}+168x^{11}-91x^{10}-63x^9+49x^8+125x^7+21x^6+133x^5+140x^4+42x^3+35x^2-133x+129$	7	-1	2T1, 7T1	14	-1	
$x^{14}+126x^{13}-14x^{12}+168x^{11}-91x^{10}-63x^9+49x^8-169x^7+21x^6+133x^5+140x^4+42x^3+35x^2-133x+31$	7	-1	2T1, 7T1	14	-1	
$x^{14}+126x^{13}-14x^{12}+168x^{11}-91x^{10}-63x^9+49x^8-120x^7+21x^6+133x^5+140x^4+42x^3+35x^2-133x-67$	7	-1	2T1, 7T1	14	-1	
$x^{14}+70x^7+49$	7	0	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+168x^8+48x^7+112x^6-77x^5-49x^4-56x^3+63x^2-105x-25$	7	0	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 + 97x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x - 123$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 + 146x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x + 122$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 - 148x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x + 24$	7	0	2T1	1	-1	
$x^{14} + 98x^7 + 98$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 - 50x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x + 171$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 + 97x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x + 24$	7	0	2T1, 7T4	2	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 + 146x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x - 74$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 - 148x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x + 171$	7	0	2T1	1	-1	
$x^{14} + 35x^7 + 98$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 - 50x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x - 25$	7	0	2T1	1	-1	
$x^{14} + 21x^7 + 49$	7	0	2T1	1	-1	
$x^{14} + 49x^8 + 98$	7	0	2T1, 7T4	2	-1	
$x^{14} + 49x^7 + 98$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 - 50x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x + 122$	7	0	2T1	1	-1	
$x^{14} + 28x^7 + 49$	7	0	2T1	1	-1	
$x^{14} + 42x^{13} + 91x^{12} + 84x^{11} - 49x^{10} + 35x^9 + 168x^8 + 48x^7 + 112x^6 - 77x^5 - 49x^4 - 56x^3 + 63x^2 - 105x - 74$	7	0	2T1	1	-1	
$x^{14} + 49x^8 + 49$	7	0	2T1, 7T4	2	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+77x^7+49$	7	0	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+168x^8+48x^7+112x^6-77x^5-49x^4-56x^3+63x^2-105x+73$	7	0	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+168x^8+97x^7+112x^6-77x^5-49x^4-56x^3+63x^2-105x-25$	7	0	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+168x^8+48x^7+112x^6-77x^5-49x^4-56x^3+63x^2-105x-123$	7	0	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+168x^8+97x^7+112x^6-77x^5-49x^4-56x^3+63x^2-105x+122$	7	0	2T1	1	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+168x^8+146x^7+112x^6-77x^5-49x^4-56x^3+63x^2-105x+24$	7	0	2T1	1	-1	
$x^{14}+98x^8+98$	7	0	2T1, 7T4	2	-1	
$x^{14}+42x^{13}+91x^{12}+84x^{11}-49x^{10}+35x^9+168x^8-148x^7+112x^6-77x^5-49x^4-56x^3+63x^2-105x+73$	7	0	2T1	1	-1	
$x^{14}+14x^7+98$	7	0	2T1, 7T4	2	-1	
$x^{14}+7x+14$	14	-6	2T1	1	-1	
$x^{14}+7x+28$	14	-6	2T1	1	-1	
$x^{14}+7x+7$	14	-6	2T1	1	-1	
$x^{14}+7x+21$	14	-6	2T1	1	-1	
$x^{14}+7x+42$	14	-6	2T1	1	-1	
$x^{14}+7x+35$	14	-6	2T1	1	-1	
$x^{14}+14x^2+7$	14	-5	2T1, 7T4	2	-1	
$x^{14}+28x^2+7$	14	-5	2T1, 7T4	2	-1	
$x^{14}+42x^2+7$	14	-5	2T1, 7T4	2	-1	
$x^{14}+7x^2+7$	14	-5	2T1, 7T4	2	-1	
$x^{14}+21x^2+7$	14	-5	2T1, 7T4	2	-1	
$x^{14}+35x^2+7$	14	-5	2T1, 7T4	2	-1	
$x^{14}+42x^2+21$	14	-5	2T1, 7T4	2	-1	
$x^{14}+35x^2+21$	14	-5	2T1, 7T4	2	1	
$x^{14}+28x^2+21$	14	-5	2T1, 7T4	2	-1	
$x^{14}+21x^2+21$	14	-5	2T1, 7T4	2	1	
$x^{14}+14x^2+21$	14	-5	2T1, 7T4	2	-1	
$x^{14}+7x^2+21$	14	-5	2T1, 7T4	2	1	
$x^{14}+7x^3+28$	14	-4	2T1	1	-1	
$x^{14}+7x^3+14$	14	-4	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+7x^3+7$	14	-4	2T1	1	-1	
$x^{14}+7x^3+21$	14	-4	2T1	1	-1	
$x^{14}+7x^3+35$	14	-4	2T1	1	-1	
$x^{14}+7x^3+42$	14	-4	2T1	1	-1	
$x^{14}+7x^4+14$	14	-3	2T1, 7T3	2	-1	
$x^{14}+7x^4+28$	14	-3	2T1, 7T3	2	-1	
$x^{14}+21x^4+14$	14	-3	2T1, 7T4	2	-1	
$x^{14}+7x^4+7$	14	-3	2T1, 7T3	2	-1	
$x^{14}+21x^4+7$	14	-3	2T1, 7T4	2	-1	
$x^{14}+21x^4+28$	14	-3	2T1, 7T4	2	-1	
$x^{14}+21x^4+42$	14	-3	2T1, 7T3	2	-1	
$x^{14}+21x^4+35$	14	-3	2T1, 7T3	2	1	
$x^{14}+7x^4+35$	14	-3	2T1, 7T4	2	-1	
$x^{14}+21x^4+21$	14	-3	2T1, 7T3	2	1	
$x^{14}+7x^4+42$	14	-3	2T1, 7T4	2	-1	
$x^{14}+7x^4+21$	14	-3	2T1, 7T4	2	1	
$x^{14}+14x^5+7$	14	-2	2T1	1	-1	
$x^{14}+21x^5+7$	14	-2	2T1	1	-1	
$x^{14}+7x^5+7$	14	-2	2T1	1	-1	
$x^{14}+7x^5+21$	14	-2	2T1	1	-1	
$x^{14}+14x^5+21$	14	-2	2T1	1	-1	
$x^{14}+21x^5+21$	14	-2	2T1	1	-1	
$x^{14}+7x^6+28$	14	-1	2T1, 7T2	2	-1	
$x^{14}+7x^6+14$	14	-1	2T1, 7T4	2	-1	
$x^{14}+21x^6+28$	14	-1	2T1, 7T4	2	-1	
$x^{14}+7x^6+7$	14	-1	2T1, 7T4	2	-1	
$x^{14}+21x^6+7$	14	-1	2T1, 7T4	2	-1	
$x^{14}+21x^6+14$	14	-1	2T1, 7T2	14	-1	
$x^{14}-91x^{12}-14x^7+84x^6+56$	14	-1	2T1	7	-1	
$x^{14}-91x^{12}-28x^7+84x^6-140$	14	-1	2T1	7	-1	
$x^{14}-91x^{12}-42x^7+84x^6+105$	14	-1	2T1	7	-1	
$x^{14}+21x^6+35$	14	-1	2T1, 7T2	2	1	
$x^{14}+21x^6+42$	14	-1	2T1, 7T4	2	-1	
$x^{14}+7x^6+42$	14	-1	2T1, 7T4	2	1	
$x^{14}+21x^6+21$	14	-1	2T1, 7T4	2	-1	
$x^{14}+7x^6+35$	14	-1	2T1, 7T4	2	1	
$x^{14}+7x^6+21$	14	-1	2T1, 7T2	14	-1	
$x^{14}-77x^{12}-91x^7-140x^6-28$	14	-1	2T1	7	1	
$x^{14}-77x^{12}+161x^7-140x^6-77$	14	-1	2T1	7	-1	
$x^{14}-77x^{12}+70x^7-140x^6+70$	14	-1	2T1	7	1	
$x^{14}+35x^8+7$	14	1	2T1, 7T4	2	-1	
$x^{14}-14x^8-14x^7+49x^2+98x+56$	14	1	2T1	1	-1	
$x^{14}-14x^8-28x^7+49x^2-147x-140$	14	1	2T1	1	-1	
$x^{14}-14x^8-42x^7+49x^2-49x+105$	14	1	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+21x^8+7$	14	1	2T1, 7T4	2	-1	
$x^{14}-28x^8-14x^7-147x^2-147x+56$	14	1	2T1	1	-1	
$x^{14}-28x^8-28x^7-147x^2+49x-140$	14	1	2T1	1	-1	
$x^{14}-28x^8-42x^7-147x^2-98x+105$	14	1	2T1	1	-1	
$x^{14}+7x^8+7$	14	1	2T1, 7T3	2	-1	
$x^{14}-42x^8-14x^7+98x^2-49x+56$	14	1	2T1	1	-1	
$x^{14}-42x^8-28x^7+98x^2-98x-140$	14	1	2T1	1	-1	
$x^{14}-42x^8-42x^7+98x^2-147x+105$	14	1	2T1	1	-1	
$x^{14}+42x^8+7$	14	1	2T1, 7T4	2	-1	
$x^{14}-56x^8-14x^7+98x^2+49x+56$	14	1	2T1	1	-1	
$x^{14}-56x^8-28x^7+98x^2+98x-140$	14	1	2T1	1	-1	
$x^{14}-56x^8-42x^7+98x^2+147x+105$	14	1	2T1	1	-1	
$x^{14}+28x^8+7$	14	1	2T1, 7T3	2	-1	
$x^{14}-70x^8-14x^7-147x^2+147x+56$	14	1	2T1	1	-1	
$x^{14}-70x^8-28x^7-147x^2-49x-140$	14	1	2T1	1	-1	
$x^{14}-70x^8-42x^7-147x^2+98x+105$	14	1	2T1	1	-1	
$x^{14}+3x^7+18$	14	1	2T1, 7T3	2	-1	
$x^{14}+y^7+2$	14	1	2T1	1	-1	
$x^{14}+y^7+44$	14	1	2T1	1	-1	
$x^{14}+2x^7+8$	14	1	2T1	1	-1	
$x^{14}+7x^8+21$	14	1	2T1, 7T4	2	-1	
$x^{14}-91x^8-91x^7+98x^2-147x-28$	14	1	2T1	1	1	
$x^{14}-91x^8+161x^7+98x^2+49x-77$	14	1	2T1	1	-1	
$x^{14}-91x^8+70x^7+98x^2-98x+70$	14	1	2T1	1	1	
$x^{14}+y^7+30$	14	1	2T1, 7T4	2	-1	
$x^{14}+y^7+9$	14	1	2T1	1	1	
$x^{14}+2x^7+43$	14	1	2T1	1	-1	
$x^{14}+2x^7+22$	14	1	2T1	1	1	
$x^{14}+21x^8+21$	14	1	2T1, 7T3	2	-1	
$x^{14}+70x^8-91x^7-147x^2-98x-28$	14	1	2T1	1	1	
$x^{14}+70x^8+161x^7-147x^2+147x-77$	14	1	2T1	1	-1	
$x^{14}+70x^8+70x^7-147x^2+49x+70$	14	1	2T1	1	1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+28x^8+21$	14	1	2T1, 7T4	2	-1	
$x^{14}-21x^8-91x^7-147x^2+98x-28$	14	1	2T1	1	1	
$x^{14}-21x^8+161x^7-147x^2-147x-77$	14	1	2T1	1	-1	
$x^{14}-21x^8+70x^7-147x^2-49x+70$	14	1	2T1	1	1	
$x^{14}+35x^8+21$	14	1	2T1, 7T3	2	-1	
$x^{14}-112x^8-91x^7+49x^2-49x-28$	14	1	2T1	1	1	
$x^{14}-112x^8+161x^7+49x^2-98x-77$	14	1	2T1	1	-1	
$x^{14}-112x^8+70x^7+49x^2-147x+70$	14	1	2T1	1	1	
$x^{14}+42x^8+21$	14	1	2T1, 7T3	2	-1	
$x^{14}+140x^8-91x^7+98x^2+147x-28$	14	1	2T1	1	1	
$x^{14}+140x^8+161x^7+98x^2-49x-77$	14	1	2T1	1	-1	
$x^{14}+140x^8+70x^7+98x^2+98x+70$	14	1	2T1	1	1	
$x^{14}+7x^9+28$	14	2	2T1	1	-1	
$x^{14}-14x^9-14x^7+49x^4+98x^2+56$	14	2	2T1	1	-1	
$x^{14}-14x^9-28x^7+49x^4-147x^2-140$	14	2	2T1	1	-1	
$x^{14}-14x^9-42x^7+49x^4-49x^2+105$	14	2	2T1	1	-1	
$x^{14}-14x^9-56x^7+49x^4+49x^2+105$	14	2	2T1	1	-1	
$x^{14}-14x^9-70x^7+49x^4+147x^2-140$	14	2	2T1	1	-1	
$x^{14}-14x^9-84x^7+49x^4-98x^2+56$	14	2	2T1	1	-1	
$x^{14}+7x^9+14$	14	2	2T1	1	-1	
$x^{14}-28x^9-14x^7-147x^4-147x^2+56$	14	2	2T1	1	-1	
$x^{14}-28x^9-28x^7-147x^4+49x^2-140$	14	2	2T1	1	-1	
$x^{14}-28x^9-42x^7-147x^4-98x^2+105$	14	2	2T1	1	-1	
$x^{14}-28x^9-56x^7-147x^4+98x^2+105$	14	2	2T1	1	-1	
$x^{14}-28x^9-70x^7-147x^4-49x^2-140$	14	2	2T1	1	-1	
$x^{14}-28x^9-84x^7-147x^4+147x^2+56$	14	2	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+7x^9+7$	14	2	2T1	1	-1	
$x^{14}-42x^9-14x^7+98x^4-49x^2+56$	14	2	2T1	1	-1	
$x^{14}-42x^9-28x^7+98x^4-98x^2-140$	14	2	2T1	1	-1	
$x^{14}-42x^9-42x^7+98x^4-147x^2+105$	14	2	2T1	1	-1	
$x^{14}-42x^9-56x^7+98x^4+147x^2+105$	14	2	2T1	1	-1	
$x^{14}-42x^9-70x^7+98x^4+98x^2-140$	14	2	2T1	1	-1	
$x^{14}-42x^9-84x^7+98x^4+49x^2+56$	14	2	2T1	1	-1	
$x^{14}+7x^9+21$	14	2	2T1	1	-1	
$x^{14}-91x^9-91x^7+98x^4-147x^2-28$	14	2	2T1	1	-1	
$x^{14}-91x^9+161x^7+98x^4+49x^2-77$	14	2	2T1	1	-1	
$x^{14}-91x^9+70x^7+98x^4-98x^2+70$	14	2	2T1	1	-1	
$x^{14}-91x^9-21x^7+98x^4+98x^2+70$	14	2	2T1	1	-1	
$x^{14}-91x^9-112x^7+98x^4-49x^2-77$	14	2	2T1	1	-1	
$x^{14}-91x^9+140x^7+98x^4+147x^2-28$	14	2	2T1	1	-1	
$x^{14}+7x^9+35$	14	2	2T1	1	-1	
$x^{14}+161x^9-91x^7+49x^4+49x^2-28$	14	2	2T1	1	-1	
$x^{14}+161x^9+161x^7+49x^4+98x^2-77$	14	2	2T1	1	-1	
$x^{14}+161x^9+70x^7+49x^4+147x^2+70$	14	2	2T1	1	-1	
$x^{14}+161x^9-21x^7+49x^4-147x^2+70$	14	2	2T1	1	-1	
$x^{14}+161x^9-112x^7+49x^4-98x^2-77$	14	2	2T1	1	-1	
$x^{14}+161x^9+140x^7+49x^4-49x^2-28$	14	2	2T1	1	-1	
$x^{14}+7x^9+42$	14	2	2T1	1	-1	
$x^{14}+70x^9-91x^7-147x^4-98x^2-28$	14	2	2T1	1	-1	
$x^{14}+70x^9+161x^7-147x^4+147x^2-77$	14	2	2T1	1	-1	
$x^{14}+70x^9+70x^7-147x^4+49x^2+70$	14	2	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}+70x^9-21x^7-147x^4-49x^2+70$	14	2	2T1	1	-1	
$x^{14}+70x^9-112x^7-147x^4-147x^2-77$	14	2	2T1	1	-1	
$x^{14}+70x^9+140x^7-147x^4+98x^2-28$	14	2	2T1	1	-1	
$x^{14}+21x^{10}+28$	14	3	2T1, 7T4	2	-1	
$x^{14}-14x^{10}-14x^7+49x^6+98x^3+56$	14	3	2T1	1	-1	
$x^{14}-14x^{10}-28x^7+49x^6-147x^3-140$	14	3	2T1	1	-1	
$x^{14}-14x^{10}-42x^7+49x^6-49x^3+105$	14	3	2T1	1	-1	
$x^{14}+21x^{10}+7$	14	3	2T1, 7T4	2	-1	
$x^{14}-28x^{10}-14x^7-147x^6-147x^3+56$	14	3	2T1	1	-1	
$x^{14}-28x^{10}-28x^7-147x^6+49x^3-140$	14	3	2T1	1	-1	
$x^{14}-28x^{10}-42x^7-147x^6-98x^3+105$	14	3	2T1	1	-1	
$x^{14}+7x^{10}+7$	14	3	2T1, 7T4	2	-1	
$x^{14}-42x^{10}-14x^7+98x^6-49x^3+56$	14	3	2T1	1	-1	
$x^{14}-42x^{10}-28x^7+98x^6-98x^3-140$	14	3	2T1	1	-1	
$x^{14}-42x^{10}-42x^7+98x^6-147x^3+105$	14	3	2T1	1	-1	
$x^{14}+21x^{10}+14$	14	3	2T1, 7T4	2	-1	
$x^{14}-56x^{10}-14x^7+98x^6+49x^3+56$	14	3	2T1	1	-1	
$x^{14}-56x^{10}-28x^7+98x^6+98x^3-140$	14	3	2T1	1	-1	
$x^{14}-56x^{10}-42x^7+98x^6+147x^3+105$	14	3	2T1	1	-1	
$x^{14}+7x^{10}+28$	14	3	2T1, 7T4	2	-1	
$x^{14}-70x^{10}-14x^7-147x^6+147x^3+56$	14	3	2T1	1	-1	
$x^{14}-70x^{10}-28x^7-147x^6-49x^3-140$	14	3	2T1	1	-1	
$x^{14}-70x^{10}-42x^7-147x^6+98x^3+105$	14	3	2T1	1	-1	
$x^{14}+7x^{10}+14$	14	3	2T1, 7T4	2	-1	
$x^{14}-84x^{10}-14x^7+49x^6-98x^3+56$	14	3	2T1	1	-1	
$x^{14}-84x^{10}-28x^7+49x^6+147x^3-140$	14	3	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14}-84x^{10}-42x^7+49x^6+49x^3+105$	14	3	2T1	1	-1	
$x^{14}+7x^{10}+21$	14	3	2T1, 7T4	2	-1	
$x^{14}-91x^{10}-91x^7+98x^6-147x^3-28$	14	3	2T1	1	1	
$x^{14}-91x^{10}+161x^7+98x^6+49x^3-77$	14	3	2T1	1	-1	
$x^{14}-91x^{10}+70x^7+98x^6-98x^3+70$	14	3	2T1	1	1	
$x^{14}+7x^{10}+42$	14	3	2T1, 7T4	2	-1	
$x^{14}+161x^{10}-91x^7+49x^6+49x^3-28$	14	3	2T1	1	1	
$x^{14}+161x^{10}+161x^7+49x^6+98x^3-77$	14	3	2T1	1	-1	
$x^{14}+161x^{10}+70x^7+49x^6+147x^3+70$	14	3	2T1	1	1	
$x^{14}+21x^{10}+21$	14	3	2T1, 7T4	2	-1	
$x^{14}+70x^{10}-91x^7-147x^6-98x^3-28$	14	3	2T1	1	1	
$x^{14}+70x^{10}+161x^7-147x^6+147x^3-77$	14	3	2T1	1	-1	
$x^{14}+70x^{10}+70x^7-147x^6+49x^3+70$	14	3	2T1	1	1	
$x^{14}+7x^{10}+35$	14	3	2T1, 7T4	2	-1	
$x^{14}-21x^{10}-91x^7-147x^6+98x^3-28$	14	3	2T1	1	1	
$x^{14}-21x^{10}+161x^7-147x^6-147x^3-77$	14	3	2T1	1	-1	
$x^{14}-21x^{10}+70x^7-147x^6-49x^3+70$	14	3	2T1	1	1	
$x^{14}+21x^{10}+35$	14	3	2T1, 7T4	2	-1	
$x^{14}-112x^{10}-91x^7+49x^6-49x^3-28$	14	3	2T1	1	1	
$x^{14}-112x^{10}+161x^7+49x^6-98x^3-77$	14	3	2T1	1	-1	
$x^{14}-112x^{10}+70x^7+49x^6-147x^3+70$	14	3	2T1	1	1	
$x^{14}+21x^{10}+42$	14	3	2T1, 7T4	2	-1	
$x^{14}+140x^{10}-91x^7+98x^6+147x^3-28$	14	3	2T1	1	1	
$x^{14}+140x^{10}+161x^7+98x^6-49x^3-77$	14	3	2T1	1	-1	
$x^{14}+140x^{10}+70x^7+98x^6+98x^3+70$	14	3	2T1	1	1	
$x^{14}+14x^{11}+7$	14	4	2T1	1	-1	
$x^{14}-14x^{11}+49x^8-14x^7+98x^4+56$	14	4	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} - 14x^{11} + 49x^8 - 28x^7 - 147x^4 - 140$	14	4	2T1	1	-1	
$x^{14} - 14x^{11} + 49x^8 - 42x^7 - 49x^4 + 105$	14	4	2T1	1	-1	
$x^{14} - 14x^{11} + 49x^8 - 56x^7 + 49x^4 + 105$	14	4	2T1	1	-1	
$x^{14} - 14x^{11} + 49x^8 - 70x^7 + 147x^4 - 140$	14	4	2T1	1	-1	
$x^{14} - 14x^{11} + 49x^8 - 84x^7 - 98x^4 + 56$	14	4	2T1	1	-1	
$x^{14} + 21x^{11} + 7$	14	4	2T1	1	-1	
$x^{14} - 28x^{11} - 147x^8 - 14x^7 - 147x^4 + 56$	14	4	2T1	1	-1	
$x^{14} - 28x^{11} - 147x^8 - 28x^7 + 49x^4 - 140$	14	4	2T1	1	-1	
$x^{14} - 28x^{11} - 147x^8 - 42x^7 - 98x^4 + 105$	14	4	2T1	1	-1	
$x^{14} - 28x^{11} - 147x^8 - 56x^7 + 98x^4 + 105$	14	4	2T1	1	-1	
$x^{14} - 28x^{11} - 147x^8 - 70x^7 - 49x^4 - 140$	14	4	2T1	1	-1	
$x^{14} - 28x^{11} - 147x^8 - 84x^7 + 147x^4 + 56$	14	4	2T1	1	-1	
$x^{14} + 7x^{11} + 7$	14	4	2T1	1	-1	
$x^{14} - 42x^{11} + 98x^8 - 14x^7 - 49x^4 + 56$	14	4	2T1	1	-1	
$x^{14} - 42x^{11} + 98x^8 - 28x^7 - 98x^4 - 140$	14	4	2T1	1	-1	
$x^{14} - 42x^{11} + 98x^8 - 42x^7 - 147x^4 + 105$	14	4	2T1	1	-1	
$x^{14} - 42x^{11} + 98x^8 - 56x^7 + 147x^4 + 105$	14	4	2T1	1	-1	
$x^{14} - 42x^{11} + 98x^8 - 70x^7 + 98x^4 - 140$	14	4	2T1	1	-1	
$x^{14} - 42x^{11} + 98x^8 - 84x^7 + 49x^4 + 56$	14	4	2T1	1	-1	
$x^{14} + 7x^{11} + 21$	14	4	2T1	1	-1	
$x^{14} - 91x^{11} + 98x^8 - 91x^7 - 147x^4 - 28$	14	4	2T1	1	-1	
$x^{14} - 91x^{11} + 98x^8 + 161x^7 + 49x^4 - 77$	14	4	2T1	1	-1	
$x^{14} - 91x^{11} + 98x^8 + 70x^7 - 98x^4 + 70$	14	4	2T1	1	-1	
$x^{14} - 91x^{11} + 98x^8 - 21x^7 + 98x^4 + 70$	14	4	2T1	1	-1	
$x^{14} - 91x^{11} + 98x^8 - 112x^7 - 49x^4 - 77$	14	4	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} - 91x^{11} + 98x^8 + 140x^7 + 147x^4 - 28$	14	4	2T1	1	-1	
$x^{14} + 14x^{11} + 21$	14	4	2T1	1	-1	
$x^{14} + 161x^{11} + 49x^8 - 91x^7 + 49x^4 - 28$	14	4	2T1	1	-1	
$x^{14} + 161x^{11} + 49x^8 + 161x^7 + 98x^4 - 77$	14	4	2T1	1	-1	
$x^{14} + 161x^{11} + 49x^8 + 70x^7 + 147x^4 + 70$	14	4	2T1	1	-1	
$x^{14} + 161x^{11} + 49x^8 - 21x^7 - 147x^4 + 70$	14	4	2T1	1	-1	
$x^{14} + 161x^{11} + 49x^8 - 112x^7 - 98x^4 - 77$	14	4	2T1	1	-1	
$x^{14} + 161x^{11} + 49x^8 + 140x^7 - 49x^4 - 28$	14	4	2T1	1	-1	
$x^{14} + 21x^{11} + 21$	14	4	2T1	1	-1	
$x^{14} + 70x^{11} - 147x^8 - 91x^7 - 98x^4 - 28$	14	4	2T1	1	-1	
$x^{14} + 70x^{11} - 147x^8 + 161x^7 + 147x^4 - 77$	14	4	2T1	1	-1	
$x^{14} + 70x^{11} - 147x^8 + 70x^7 + 49x^4 + 70$	14	4	2T1	1	-1	
$x^{14} + 70x^{11} - 147x^8 - 21x^7 - 49x^4 + 70$	14	4	2T1	1	-1	
$x^{14} + 70x^{11} - 147x^8 - 112x^7 - 147x^4 - 77$	14	4	2T1	1	-1	
$x^{14} + 70x^{11} - 147x^8 + 140x^7 + 98x^4 - 28$	14	4	2T1	1	-1	
$x^{14} + 21x^{12} + 14$	14	5	2T1, 7T3	2	-1	
$x^{14} - 14x^{12} + 49x^{10} - 14x^7 + 98x^5 + 56$	14	5	2T1	1	-1	
$x^{14} - 14x^{12} + 49x^{10} - 28x^7 - 147x^5 - 140$	14	5	2T1	1	-1	
$x^{14} - 14x^{12} + 49x^{10} - 42x^7 - 49x^5 + 105$	14	5	2T1	1	-1	
$x^{14} + 21x^{12} + 7$	14	5	2T1, 7T3	2	-1	
$x^{14} - 28x^{12} - 147x^{10} - 14x^7 - 147x^5 + 56$	14	5	2T1	1	-1	
$x^{14} - 28x^{12} - 147x^{10} - 28x^7 + 49x^5 - 140$	14	5	2T1	1	-1	
$x^{14} - 28x^{12} - 147x^{10} - 42x^7 - 98x^5 + 105$	14	5	2T1	1	-1	
$x^{14} + 7x^{12} + 7$	14	5	2T1, 7T2	2	-1	
$x^{14} - 42x^{12} + 98x^{10} - 14x^7 - 49x^5 + 56$	14	5	2T1	1	-1	
$x^{14} - 42x^{12} + 98x^{10} - 28x^7 - 98x^5 - 140$	14	5	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} - 42x^{12} + 98x^{10} - 42x^7 - 147x^5 + 105$	14	5	2T1	1	-1	
$x^{14} + 42x^{12} + 7$	14	5	2T1, 7T1	14	-1	
$x^{14} + 21x^{12} + 77$	14	5	2T1, 7T1	14	-1	
$x^{14} + 21x^{12} + 28$	14	5	2T1, 7T1	14	-1	
$x^{14} + 42x^{12} + 56$	14	5	2T1, 7T1	14	-1	
$x^{14} - 56x^{12} + 98x^{10} - 42$	14	5	2T1, 7T1	14	-1	
$x^{14} - 56x^{12} + 98x^{10} - 140$	14	5	2T1, 7T1	14	-1	
$x^{14} + 35x^{12} + 63$	14	5	2T1, 7T1	14	-1	
$x^{14} - 56x^{12} + 98x^{10} - 14x^7 + 49x^5 + 56$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 14x^7 + 49x^5 - 42$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 14x^7 + 49x^5 - 140$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 14x^7 + 49x^5 + 105$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 14x^7 + 49x^5 + 7$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 14x^7 + 49x^5 - 91$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 14x^7 + 49x^5 + 154$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 28x^7 + 98x^5 - 140$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 28x^7 + 98x^5 + 105$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 28x^7 + 98x^5 + 7$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 28x^7 + 98x^5 - 91$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 28x^7 + 98x^5 + 154$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 28x^7 + 98x^5 + 56$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 28x^7 + 98x^5 - 42$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 42x^7 + 147x^5 + 105$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 42x^7 + 147x^5 + 7$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 42x^7 + 147x^5 - 91$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 42x^7 + 147x^5 + 154$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 42x^7 + 147x^5 + 56$	14	5	2T1	7	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} - 56x^{12} + 98x^{10} - 42x^7 + 147x^5 - 42$	14	5	2T1	7	-1	
$x^{14} - 56x^{12} + 98x^{10} - 42x^7 + 147x^5 - 140$	14	5	2T1	7	-1	
$x^{14} + 7x^{12} + 14$	14	5	2T1, 7T4	2	-1	
$x^{14} - 70x^{12} - 147x^{10} - 14x^7 + 147x^5 + 56$	14	5	2T1	1	-1	
$x^{14} - 70x^{12} - 147x^{10} - 28x^7 - 49x^5 - 140$	14	5	2T1	1	-1	
$x^{14} - 70x^{12} - 147x^{10} - 42x^7 + 98x^5 + 105$	14	5	2T1	1	-1	
$x^{14} + 7x^{12} + 28$	14	5	2T1, 7T4	2	-1	
$x^{14} - 84x^{12} + 49x^{10} - 14x^7 - 98x^5 + 56$	14	5	2T1	1	-1	
$x^{14} - 84x^{12} + 49x^{10} - 28x^7 + 147x^5 - 140$	14	5	2T1	1	-1	
$x^{14} + 14x^{13} + 7$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 14$	14	6	2T1	1	-1	
$x^{14} + 21x^{13} + 28$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 56$	14	6	2T1	1	-1	
$x^{14} - 14x^{13} + 49x^{12} - 42$	14	6	2T1	1	-1	
$x^{14} - 14x^{13} + 49x^{12} - 140$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 63$	14	6	2T1	1	-1	
$x^{14} + 21x^{13} + 7$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 77$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 28$	14	6	2T1	1	-1	
$x^{14} + 21x^{13} + 56$	14	6	2T1	1	-1	
$x^{14} - 28x^{13} - 147x^{12} - 42$	14	6	2T1	1	-1	
$x^{14} - 28x^{13} - 147x^{12} - 140$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 63$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 7$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 77$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 28$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 56$	14	6	2T1	1	-1	
$x^{14} - 42x^{13} + 98x^{12} - 42$	14	6	2T1	1	-1	
$x^{14} - 42x^{13} + 98x^{12} - 140$	14	6	2T1	1	-1	
$x^{14} + 21x^{13} + 63$	14	6	2T1	1	-1	
$x^{14} - 91x^{13} + 98x^{12} - 126$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 21$	14	6	2T1	1	-1	
$x^{14} - 91x^{13} + 98x^{12} + 168$	14	6	2T1	1	-1	
$x^{14} - 91x^{13} + 98x^{12} - 28$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 84$	14	6	2T1	1	-1	
$x^{14} + 21x^{13} + 91$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 70$	14	6	2T1	1	-1	
$x^{14} + 161x^{13} + 49x^{12} - 126$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 21$	14	6	2T1	1	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} + 161x^{13} + 49x^{12} + 168$	14	6	2T1	1	-1	
$x^{14} + 161x^{13} + 49x^{12} - 28$	14	6	2T1	1	-1	
$x^{14} + 21x^{13} + 84$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 91$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 42$	14	6	2T1	1	-1	
$x^{14} + 70x^{13} - 147x^{12} - 126$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 35$	14	6	2T1	1	-1	
$x^{14} + 70x^{13} - 147x^{12} + 168$	14	6	2T1	1	-1	
$x^{14} + 70x^{13} - 147x^{12} - 28$	14	6	2T1	1	-1	
$x^{14} + 7x^{13} + 84$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 91$	14	6	2T1	1	-1	
$x^{14} + 14x^{13} + 42$	14	6	2T1	1	-1	
$x^{14} + 98x^2 + 14$	14	7	2T1, 7T4	2	-1	
$x^{14} + 98x^2 + 28$	14	7	2T1, 7T4	2	-1	
$x^{14} + 49x^2 + 63$	14	7	2T1, 7T4	2	-1	
$x^{14} + 49x^2 + 7$	14	7	2T1, 7T4	2	-1	
$x^{14} + 49x^2 + 14$	14	7	2T1, 7T4	2	-1	
$x^{14} + 49x^2 + 28$	14	7	2T1, 7T4	2	-1	
$x^{14} + 49x^2 + 56$	14	7	2T1, 7T4	2	-1	
$x^{14} + 98x + 56$	14	7	2T1	1	-1	
$x^{14} - 14x^7 - 42$	14	7	2T1	1	-1	
$x^{14} - 14x^7 - 140$	14	7	2T1	1	-1	
$x^{14} + 49x + 63$	14	7	2T1	1	-1	
$x^{14} + 98x + 7$	14	7	2T1	1	-1	
$x^{14} + 49x + 14$	14	7	2T1	1	-1	
$x^{14} + 21x^7 + 28$	14	7	2T1	1	-1	
$x^{14} - 28x^7 - 140$	14	7	2T1	1	-1	
$x^{14} + 98x + 63$	14	7	2T1	1	-1	
$x^{14} + 21x^7 + 7$	14	7	2T1	1	-1	
$x^{14} + 49x + 77$	14	7	2T1	1	-1	
$x^{14} + 49x + 28$	14	7	2T1	1	-1	
$x^{14} + 21x^7 + 56$	14	7	2T1	1	-1	
$x^{14} - 28x^7 - 42$	14	7	2T1	1	-1	
$x^{14} + 21x^7 + 63$	14	7	2T1	1	-1	
$x^{14} + 49x + 7$	14	7	2T1	1	-1	
$x^{14} + 98x + 77$	14	7	2T1	1	-1	
$x^{14} + 98x + 28$	14	7	2T1	1	-1	
$x^{14} + 49x + 56$	14	7	2T1	1	-1	
$x^{14} + 7x^7 + 98$	14	7	2T1	1	-1	
$x^{14} - 42x^7 - 140$	14	7	2T1	1	-1	
$x^{14} + 49x^2 + 42$	14	7	2T1, 7T4	2	1	
$x^{14} + 98x^2 + 42$	14	7	2T1, 7T4	2	-1	
$x^{14} + 49x^2 + 21$	14	7	2T1, 7T4	2	1	
$x^{14} + 98x^2 + 21$	14	7	2T1, 7T4	2	-1	
$x^{14} + 49x^3 + 84$	14	7	2T1, 7T4	2	1	
$x^{14} + 49x^2 + 84$	14	7	2T1, 7T4	2	-1	

Defining Polynomial	e	j	sgg Content	C.O.	Parity	G
$x^{14} + 49x^2 + 91$	14	7	2T1, 7T4	2	1	
$x^{14} - 91x^7 - 28$	14	7	2T1	1	-1	
$x^{14} + 98x + 84$	14	7	2T1	1	1	
$x^{14} + 21x^7 + 91$	14	7	2T1	1	-1	
$x^{14} + 49x + 70$	14	7	2T1	1	1	
$x^{14} - 91x^7 - 126$	14	7	2T1	1	-1	
$x^{14} + 49x + 21$	14	7	2T1	1	1	
$x^{14} - 91x^7 + 168$	14	7	2T1	1	-1	
$x^{14} + 49x + 91$	14	7	2T1	1	1	
$x^{14} + 49x + 42$	14	7	2T1	1	-1	
$x^{14} + 63x^7 + 49$	14	7	2T1	1	1	
$x^{14} + 98x + 21$	14	7	2T1	1	-1	
$x^{14} + 161x^7 + 168$	14	7	2T1	1	1	
$x^{14} + 161x^7 - 28$	14	7	2T1	1	-1	
$x^{14} + 21x^7 + 84$	14	7	2T1	1	1	
$x^{14} + 98x + 42$	14	7	2T1	1	-1	
$x^{14} + 70x^7 - 126$	14	7	2T1	1	1	
$x^{14} + 49x + 35$	14	7	2T1	1	-1	
$x^{14} + 70x^7 + 168$	14	7	2T1	1	1	
$x^{14} + 70x^7 - 28$	14	7	2T1	1	-1	
$x^{14} + 49x + 84$	14	7	2T1	1	1	
$x^{14} + 98x + 91$	14	7	2T1	1	-1	
$x^{14} + y + 4$	1	-13	2T1, 7T1	14	-1	
$x^{14} + 49x^{12} + 1029x^{10} + 12017x^8 + 8x^7 + 82859x^6 - 1176x^5 + 352947x^4 + 13720x^3 + 881203x^2 - 19160x + 794999$	2	-12	2T1, 7T1	14	-1	
$x^{14} + 99x^{13} + 50x^{12} - 88x^{11} - 106x^{10} + 51x^9 - 6x^8 - 19x^7 + 85x^6 + 19x^5 + 90x^4 - 27x^3 + 60x^2 + 13x - 73$	2	-12	2T1, 7T1	14	1	

References

[1] Chad Awtrey. *Dodecic Local Fields.* BiblioBazaar, 2011.

[2] Chad Awtrey. Dodecic 3-adic fields. *Int. J. Number Theory*, 08(04):933–944, 2012.

[3] Jim Brown. Local class field theory, 2008.

[4] Fernando Q. Gouvêa. *P-Adic Numbers: An Introduction.* Structure and Bonding. Springer-Verlag GmbH, 1997.

[5] John W. Jones and David P. Roberts. A database of local fields. *J. Symbolic Comput.*, 41(1):80 – 97, 2006.

[6] Serge Lang. *Algebraic Number Theory.* Applied Mathematical Sciences. Springer, 1994.