# Degree $p$ Extensions of $\mathbb{Q}_p$

Caleb Dastrup

May 2022

## 1 Introduction

The extensions of $\mathbb{Q}_p$ can be divided into three types: unramified, tamely ramified, and wildly ramified. As suggested by the name, the wildly ramified extensions are the most complicated. There are many wildly ramified extensions of a given degree, and they are much harder to classify than unramified or tamely ramified extensions. The simplest case of wildly ramified extensions is the extensions of $\mathbb{Q}_p$ of degree $p$. Information on this class of extensions is given by the local fields database. This is the case that will be treated in this paper. I first give background, and then give proofs of the main results. The extensions of degree $p$ for odd primes $p$ were first classified by Shigeru Amano in 1971. Amano's paper proves results regarding degree $p$ extensions of some finite extension $k$ of $\mathbb{Q}_p$. In this paper I specialize to the case $k = \mathbb{Q}_p$, and prove that all degree $p$ extensions of $\mathbb{Q}_p$ are generated by certain canonical polynomials. I largely follow Amano's argument in sections 1, 3, and 4 of his paper; specializing to $k = \mathbb{Q}_p$ allows me to simplify the notation and give simpler proofs of some of the results. I also fill in some steps that were assumed to be obvious to the reader.

## 2 Background

Though $\mathbb{Q}_p$ is complete, it is not algebraically closed, meaning there are some polynomials with coefficients in $\mathbb{Q}_p$ that do not have roots in $\mathbb{Q}_p$. We can generate extensions of $\mathbb{Q}_p$ by adjoining roots of polynomials: for an irreducible polynomial $f(x)$ of degree $n > 1$, we can construct a field that contains $\mathbb{Q}_p$, a root $\alpha$ of $f$, and all other elements required of a field, i.e. sums $\sum_{i=0}^{n-1} a_i \alpha^i$ where $a_i \in \mathbb{Q}_p$. There is even a field which contains roots of all polynomials with coefficients in $\mathbb{Q}_p$. This is the algebraic closure of $\mathbb{Q}_p$, denoted $\overline{\mathbb{Q}_p}$. The absolute value defined on $\mathbb{Q}_p$ can be uniquely extended to $\overline{\mathbb{Q}_p}$, as can the $p$-adic valuation $v$. The following properties of the valuation will be used repeatedly: $v(ab) = v(a) + v(b)$ and $v(a+b) \geq \min(v(a), v(b))$, with equality if $v(a) \neq v(b)$. In particular, if we have a sum $a_0 + ... + a_n$ where each term has distinct valuation, then $v(a_0 + ... + a_n) = \min(v(a_0), ..., v(a_n))$.

When we extend $\mathbb{Q}_p$, the valuation can take on more values. The $p$-adic valuation has only integer values on $\mathbb{Q}_p$, but in $\mathbb{Q}_p(\sqrt{p})$, where a root of $x^2 - p$ has been added to $\mathbb{Q}_p$, $v(\sqrt{p}) = \frac{1}{2}$. In a finite extension of $\mathbb{Q}_p$ the valuations are integer multiples of $\frac{1}{e}$ for some positive integer $e$. This integer is called the ramification index. An element $\pi$ with the minimum possible positive valuation is called a uniformizer of the extension field. The residue field of an extension $K$ is the field $K/\pi K$, where $\pi$ is a uniformizer. The residue field can be thought of as describing the coefficients which appear in the digit expansions of elements of $K$. There is one unramified extension of each degree.

Unramified extensions are those with $e = 1$, so that all the valuations are still integers. These extensions enlarge the residue field $\mathbb{F}_p$ of $\mathbb{Q}_p$ to $\mathbb{F}_{p^k}$ for some $k$.

Totally ramified extensions are those where the ramification index is the same as the degree of the extension, so that the extension is 'as ramified as possible'. Every extension of $\mathbb{Q}_p$ can be represented as a composite $(\mathbb{Q}_p(\alpha))(\beta)$ of an unramified and a totally ramified extension.

An Eisenstein polynomial is a monic polynomial $x^n + \sum_{i=0}^{n-1} a_i x^i$ with $v(a_0) = 1$, $v(a_i) \geq 1$ for all $i$ at least 1. All Eisenstein polynomials are irreducibly over $\mathbb{Q}_p$.

Every totally ramified extension of $\mathbb{Q}_p$ is generated by an Eisenstein polynomial. Let the extension be of degree $d$. Then there is an element $\pi$ of valuation $\frac{1}{d}$. Let it be a root of a nonzero polynomial $f = \sum_{i=0}^{d} a_i x^i$ of degree most $d$. $\infty = v(0) = v(f(\pi)) \neq \min(v(a_i \pi^i))$, so the valuations of the terms cannot be distinct, i.e. there must be at least two terms with the minimum valuation. The valuation of $a_i \pi^i$ is $v(a_i) + \frac{i}{d} \in \frac{i}{d} + \mathbb{Z}$, so the only way two terms can have the same valuation is if they are the $a_0$ term and the $a_d \pi^d$ term. Then $a_d \neq 0$, so divide by $a_d$ to produce a monic polynomial of degree $d$. Then $1 = v(\pi^d) = v(a_0)$, so $p | a_0$ but $p^2 \not| a_0$. $v(a_i \pi^i) \geq 1$ for all $i$, so $p | a_i$ with $0 \leq i \leq d - 1$. Thus $f$ is Eisenstein. Furthermore, $\mathbb{Q}_p(\pi)$ has degree $d$, so it is the totally ramified extension.

When the ramification index is not divisible by $p$, the extension is said to be tamely ramified. There are relatively simple classifications of tamely ramified extensions.

When the ramification index is divisible by $p$, the extension is said to be wildly ramified.

There are many wildly ramified extensions of a given degree, and they are much harder to classify than unramified or tamely ramified extensions. The simplest case of wildly ramified extensions is the extensions of $\mathbb{Q}_p$ of degree $p$. This is the case that will be treated in this paper.

The following notation will be used:

Let $p$ be an odd prime. Let $v$ be the $p$-adic valuation extended to $\overline{\mathbb{Q}_p}$. Define $a \equiv b$ when $v(a) = v(b)$ and $v(a - b) > v(a)$. Let $K$ be a ramified degree $p$ extension of $\mathbb{Q}_p$.

Let $\pi$ be an element of $K$ with $v(\pi) = \frac{1}{p}$. Then as above, $\pi$ is a root of an Eisenstein polynomial. $\pi^p = up$, with $u$ a unit. Consider $\frac{\pi}{u}$. $u^p \equiv u$, so $(\frac{\pi}{u})^p =$

$\frac{\pi^p}{u^p} \equiv \frac{up}{u} = p$, so the Eisenstein polynomial of $\frac{\pi}{u}$ has constant term congruent to $-p$. Thus we can assume without loss of generality that the constant terms of the Eisenstein polynomials are $p$ mod $p^2$. This assumption will be made throughout the paper.

# 3 Invariants of $K$

Let $\pi$ be an element of $K$ with valuation $\frac{1}{p}$ and minimal polynomial $x^p - \sum_{i=1}^{p-1} a_i x^i + a_0 p$, where $a_0 \equiv 1$. $v(a_i) \geq 1$ because the polynomial is Eisenstein.

We have two cases, depending on the coefficients of the minimal polynomial.

If there is some $i$ with $1 \leq i \leq p-1$ such that $v(a_i) = 1$, then let $\lambda$ be the least such $i$. Then $f(x) = x^p - \cdots - \omega p x^\lambda - \cdots - ap$, where the the terms in the '$\cdots$' on the left have coefficients divisible by $p$ and those in the '$\cdots$' on the right have coefficients divisible by $p^2$. In particular, when we write $0 = f(\pi) = \pi^p - \cdots - \omega p \pi^\lambda - \cdots - ap$, the three terms written have smaller valuation than all omitted terms.

It is also possible that all coefficients $a_i$ with $a \leq i \leq p-1$ are divisible by $p^2$. Then $f(x) = x^p - \cdots - ap$.

$\pi$ is a root of $f(x)$, but there are $p-1$ other roots. Let $\pi_0 = \pi$, $\pi_1$, ... , $\pi_{p-1}$ be the roots of $f(x)$. We can factor $f(x)$ as $(x-\pi)(x-\pi_1)\cdots(x-\pi_{p-1})$.

Let $\Delta_i = \pi - \pi_i$.

**Lemma 1.** *All the $\Delta_i$ have the same valuation.*

*Proof.* Since $\pi^p \equiv p \equiv (\pi_i)^p = (\pi + \Delta_i)^p = \pi^p(1 + \frac{\Delta_i}{\pi})^p$, $1 + \frac{\Delta_i}{\pi} \equiv 1$, $v(\frac{\Delta_i}{\pi}) > 0$, $v(\Delta_i) > v(\pi)$.

By Taylor's expansion we have

$$f(\pi_i) = f(\pi + \Delta_i) = \sum_{j=0}^{p} \frac{f^{(j)}(\pi)}{j!} \Delta_i^j$$

Separating out the the first, second, and last terms of the sum we have

$$f(\pi_i) = f(\pi) + f'(\pi)\Delta_i + \sum_{j=2}^{p-1} \frac{f^{(j)}(\pi)}{j!} \Delta_i^j + \Delta_i^p$$

since $f^{(p)}(x) = p!$. Since $f(\pi) = f(\pi_i) = 0$, we have

$$0 = f'(\pi)\Delta_i + \sum_{j=2}^{p-1} \frac{f^{(j)}(\pi)}{j!} \Delta_i^j + \Delta_i^p$$

Consider the valuation of the terms in the summation. Terms of $f^{(j)}(\pi)$ are those of $f'(\pi)$ multiplied by an integer and divided by $j-1$ powers of $\pi$. Thus the valuation of each term of $f^{(j)}(\pi)$ is $(j-1)v(\pi)$ less than the corresponding term of $f'(\pi)$, and some terms have disappeared (since derivatives eliminate constant

terms. Since the valuation depends only on the valuation of the minimum term, $v(f^{(j)}(\pi)) \geq v(f'(\pi)) - (j-1)v(\pi)$. Then

$$v(\frac{f^{(j)}(\pi)}{j!}\Delta_i^j) = v(f^{(j)}(\pi)) + jv(\Delta_i) \geq v(f'(\pi)) - (j-1)v(\pi) + (j-1)v(\Delta_i) + v(\Delta)_i$$

$$> v(f'(\pi)) - (j-1)v(\pi) + (j-1)v(\pi) + v(\Delta)_i = v(f'(\pi)\Delta_i)$$

Thus the valuation of each term in the summation is greater than the valuation of $f'(\pi)\Delta_i$. Then for the sum of the terms to be zero, there must be more than one term with the minimum valuation, so $v(f'(\pi)\Delta_i) = v(\Delta_i^p)$, and $f'(\pi)\Delta_i \equiv -\Delta_i^p$. Then $v(\Delta_i) = \frac{v(f'(\pi))}{p-1}$, so all the $\Delta_i$s have the same valuation. □

Furthermore, we can find what this valuation is.

We have

$$f'(\pi) = p\pi^{p-1} + \sum_{i=1}^{p-1} ia_i\pi^{i-1}$$

Taking valuations, we have

$$\min(v(p\pi^{p-1}), ..., v(ia_i\pi^{i-1}), ...) = v(f'(\pi))$$

The value of the minimum depends on which case we have. In case 1 this is $v(\lambda a_\lambda \pi^{\lambda-1}) = v(\lambda\omega p\pi^{\lambda-1}) = 1 + \frac{\lambda-1}{p}$ and in case 2 this is $v(p\pi^{p-1}) = 1 + \frac{p-1}{p}$.

Thus in case 1 we have $v(\Delta_i) = \frac{v(f'(\pi))}{p-1} = \frac{\lambda+p-1}{p(p-1)}$ and in case 2 we have $v(\Delta_i) = \frac{2p-1}{p(p-1)}$. Define $C$ by $\frac{C}{p(p-1)} = v(\Delta_i) - V(\pi)$, so that $C = \lambda$ in case 1 and $C = p$ in case 2.

This implies that the valuations of the discriminants of the polynomials are $\lambda + p - 1$ and $2p - 1$, respectively, in the two cases.

We can generalize this to other elements of $K$:

**Lemma 2.** *For all $A \in K$, for any conjugate $A' \neq A$ of $A$, $v(A' - A) > \frac{C}{(p-1)p} + v(A)$ if $v(A)$ is an integer and $v(A' - A) = \frac{C}{(p-1)p} + v(A)$ otherwise.*

*Proof.* Because $K$ is a degree $p$ extension, write $A = \sum_{i=0}^{p-1} a_i\pi^i$. The valuations of the $a_i$s are integers and the valuation of $\pi$ is $\frac{1}{p}$, so all these terms have different valuation, so $v(a) = \min_{0\leq i\leq p-1}(v(a_i\pi^i))$. We have that $A' = \sum_{i=0}^{p-1} a_i\pi_j^i$ for some $j$. Then we have $A' - A = \sum_{i=0}^{p-1} a_i(\pi_j^i - \pi^i)$.

$$\pi_j^i - \pi^i = (\pi + \Delta_j)^i - \pi^i \equiv \pi^i + i\pi^{i-1}\Delta_j - \pi^i = i\Delta_j\pi^{i-1}$$

where the congruence is justified because terms with more powers of $\Delta_j$ in the binomial expansion of $(\pi + \Delta_j)^i$ have higher valuation. Then

$$v(a_i(\pi_j^i - \pi^i)) = v(a_i(\Delta_j\pi^{i-1})) = v(a_i\pi^i) + v(\Delta_j) - v(\pi) = v(a_i\pi^i) + \frac{C}{p(p-1)}$$

These valuations are distinct for all $i$, so

$$v(A' - A) = v(\sum_{i=0}^{p-1} a_i(\pi_j^i - \pi^i)) = \min_{1 \le i \le p-1}(v(a_i\pi^i) + \frac{C}{p(p-1)}) =$$

$$\min_{1 \le i \le p-1}(v(a_i\pi^i)) + \frac{C}{p(p-1)} \ge v(A) + \frac{C}{p(p-1)}$$

The minimum does not include the $i = 0$ term because this term is the same for $A$ and $A'$, and thus is cancelled in the subtraction. Thus we have equality exactly when the minimum valuation is achieved by the $a_0$ term, so that $v(A) = v(a_0)$ is an integer. □

**Theorem 1.** *$C$, $v(\Delta_i)$, and $\lambda$ depend only on $K$, not on which Eisenstein polynomial $f$ we choose to generate $K$. Thus these are invariants of $K$.*

*Proof.* Let $\alpha$ be another element of $K$ of valuation $\frac{1}{p}$. The other roots $\alpha_i$ of its minimal polynomial are its conjugates. Thus $v(\Delta_i') = v(\alpha_i - \alpha) = \frac{C}{p(p-1)} + v(\alpha_i) = \frac{C}{p(p-1)} + \frac{1}{p}$. This determines the values of $C$ and $\lambda$ for $\alpha$ by the proof of the valuation of the $\Delta_i$s, and these values are the same as those for $\pi$. □

Furthermore, in case 1, the value of $\omega$ mod $p$ is also determined by $K$.

**Lemma 3.** *For all $A$ in $K$ that are not in $\mathbb{Q}_p$, the minimal polynomial $f(x) = \sum_{i=0}^{p} a_i x^i$ of $A$ has $v(a_i) \ge \frac{C}{p} + (p-i)v(A)$ for all $i$ with $1 \le i \le p-1$.*

*Proof.* First suppose $A$ has non-integer valuation $\frac{r}{p}$. Then

$$f(x) = (x - A)(x - A_1) \cdots (x - A_{p-1})$$

so by the product rule

$$f'(x) = (x - A_1) \cdots (x - A_{p-1}) + (x - A)((x - A_2) \cdots (x - A_{p-1}))'$$

where $A_i$ is a conjugate of $A$ (another root of its minimal polynomial). When we take $f'(A)$, the second term cancels, so we have

$$f'(A) = (A - A_1)(A - A_2) \cdots (A - A_{p-1})$$

Thus we have that

$$\sum_{i=1}^{p} i a_i A^{i-1} = f'(A) = (A - A_1) \cdots (A - A_{p-1})$$

Taking valuations,

$$v(pA^{p-1} + \sum_{i=1}^{p-1} i a_i A^{i-1}) = v(A - A_1) + \cdots + v(A - A_{p-1})$$

Because all the terms in the sum in the left side have different valuations, the left side equals $\min(1+\frac{(p-1)r}{p},...,v(ia_iA^{i-1}),...)$. By Lemma 2 the right side equals $\frac{C}{p}+(p-1)v(a)=\frac{C}{p}+\frac{(p-1)r}{p}$. Thus for all $i$

$$\frac{C}{p}+\frac{(p-1)r}{p}\leq v(ia_iA^{i-1})=v(a_i)+\frac{(i-1)r}{p}$$

so

$$v(a_i)\geq\frac{C+(p-1)r}{p}-\frac{(i-1)r}{p}=\frac{C+(p-i)r}{p}=\frac{C}{p}+(p-i)r.$$

Now suppose $A$ has integer valuation. Separate $A$ into its 'constant' and '$\pi$' terms, so that we have $A=b+B$, where $b\in\mathbb{Q}_p$ and $B$ has noninteger valuation. We have $v(A)=\min(v(b),v(B))=v(b)$, since it must be an integer. The minimal polynomial of $B$ is $f(x)=x^p-\sum_{i=1}^{p-1}b_ix^i+b_0$, where the $v(b_i)\geq\frac{C}{p}+v(B)$. The minimal polynomial of $A$ is then

$$f(x-b)=(x-b)^p-\sum_{i=1}^{p-1}b_i(x-b)^i+b_0=x^i+\sum_{i=1}^{p-1}\binom{p}{i}x^ib^{p-i}+1-\sum_{i=1}^{p-1}b_i(x-b)^i+b_0$$

using the binomial theorem to expand $(x-b)^p$. Because the binomial coefficient $\binom{p}{i}$ is divisible by $p$, the valuation of the coefficient of $x^i$ in the summation on the left is $1+(p-i)v(b)\geq\frac{C}{p}+(p-1)v(A)$. If we expand $b_i(x-b)^i$ with the binomial theorem in the sum on the right, we get sums of $\binom{i}{j}b_ib^jx^{i-j}$, so the coefficient of $x^{i-j}$ has valuation $v(\binom{i}{j}b_ib^j)=v(b_i)+jv(b)\geq\frac{C}{p}+(p-i)v(B)+jv(b)>\frac{C}{p}+(p-i)v(A)+jv(A)=\frac{C}{p}+(p-(i-j))v(A)$. Thus when we collect the terms, all coefficients $a_i$ of $x^i$ with $1\leq i\leq p-1$ have valuation at least $\frac{C}{p}+(p-i)v(A)$. □

Define $N(\alpha)$ as $(-1)^p=-1$ (here we use that $p$ is odd) times the constant term of the minimal polynomial of alpha if $\alpha\notin\mathbb{Q}_p$, and $N(\alpha)=\alpha^p$ if $\alpha\in\mathbb{Q}_p$. This is called the norm of $\alpha$. Then $N(\alpha)$ is the product of $\alpha$ and all its conjugates. A key fact is that the norm is multiplicative: $N(\alpha\beta)=N(\alpha)N(\beta)$.

Let $f(x)=x^p-\sum_{i=1}^{p-1}a_ix^i-a_0$ be the minimal polynomial of $\alpha$. Then

$$\alpha^p-N(\alpha)=\alpha^p-a_0=\alpha-a_0-f(\alpha)=\sum_{i=1}^{p-1}a_i\alpha^i$$

By Lemma 3, the $a_i$s have positive valuation (and thus valuation at least 1), so $v(\alpha^p-N(\alpha))\geq 1$ if $\alpha\notin\mathbb{Q}_p$. If $\alpha\in\mathbb{Q}_p$ then $v(\alpha^p-N(\alpha))=v(0)=\infty$.

Now we can prove the following.

**Theorem 2.** *The value of $\omega$ mod $p$ is the same for all Eisenstein polynomials with a root in $K$; that is, $\omega \pmod p$ is also an invariant of $K$.*

*Proof.* Let $\pi$ and $\pi_1$ be in $K$ with valuation $\frac{1}{p}$ and minimal polynomials $x^p - \cdots - \omega p x^\lambda - \cdots - pa_0$ and $x^p - \cdots - \omega_1 p x^\lambda - \cdots - pb_0$, respectively, where $a_0 \equiv 1 \equiv b_0$, so that $\pi^p \equiv p \equiv \pi_1^p$, $\pi \equiv \pi_1$, $\pi_1 = u\pi$, $u$ a unit congruent to 1. We have

$$\pi^p - N(\pi) = \pi^p - pa_0 \equiv \omega p \pi^\lambda$$

$$\pi_1^p - N(\pi_1) = \pi_1^p - pb_0 \equiv \omega_1 p \pi_1^\lambda \equiv \omega_1 p \pi^\lambda$$

and

$$v(\omega p \pi^\lambda) = 1 + \frac{\lambda}{p} = v(\omega_1 p \pi_1^\lambda)$$

However, we have

$$p\pi^\lambda(\omega_1 - \omega) = p\pi^\lambda\omega_1 - p\pi^\lambda\omega \equiv p\pi_1^\lambda\omega_1 - p\pi^\lambda\omega_1 = (\pi_1^p - N(\pi_1)) - (\pi^p - N(\pi))$$

$$(\pi_1^p - N(\pi_1)) - (\pi^p - N(\pi)) = (\pi^p - N(\pi))((\frac{\pi}{\pi_1})^p - 1) + N(\pi)((\frac{\pi}{\pi_1})^p - \frac{N(\pi)}{N(\pi_1)}) =$$

$$(\pi^p - N(\pi))(u^p - 1) + N(\pi)(u^p - N(u))$$

$$v((\pi^p - N(\pi))(u^p - 1)) = v((u^p - 1)) + v(\omega p \pi^\lambda) = v((u^p - 1)) + 1 + \frac{\lambda}{p} > 1 + \frac{\lambda}{p}$$

$$v(N(\pi)(u^p - N(u))) = v(N(\pi)) + v(u^p - N(u)) \geq 1 + 1 > 1 + \frac{\lambda}{p}$$

Thus

$$v(p\pi^\lambda(\omega_1 - \omega)) > 1 + \frac{\lambda}{p} = v(p\pi^\lambda\omega_1)$$

so $\omega \equiv \omega_1$. □

# 4 Canonical Polynomials

Now we have proved that all polynomials defining an extension have the same value of $\lambda$ and the values of $\omega$ are congruent mod $p$. We will now prove

**Theorem 3.** *Each extension can be generated by a canonical polynomial of the form*

$$x^p - \omega p x^\lambda - p$$

$$x^p - \omega p x^{p-1} - p(1 + ap)$$

$$x^p - p(1 + ap)$$

*with $\omega$ and $\lambda$, and $a$ integers with $1 \leq \omega \leq p-1$, $1 \leq \lambda < p-1$, $0 \leq a \leq p-1$.*

*Furthermore, the extensions in the first and third cases generate distinct extensions.*

The rest of the paper gives the proof of this theorem.

We will use Krasner's Lemma:

**Lemma 4.** *For irreducible polynomial $f(x)$ in $\mathbb{Q}_p[x]$ with roots $\alpha$, $\alpha_1$,...,$\alpha_{n-1}$, if $\beta \in \Omega$ satisfies $v(\beta-\alpha) > v(\alpha_i - \alpha)$ for all $i \neq 0$, then $\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$.*

First suppose $K$ is an extension generated by $f(x) = x^p - \sum_{i=1}^{p-1} a_i x^i - ap = x^p - \cdots - \omega p x^\lambda - \cdots - ap$. Consider $g(x) = x^p - \omega' p x^\lambda - p$, where $\omega'$ is the integer between 1 and $p-1$ congruent to $\omega$. Let $\pi'_0$, $\pi'_1$,...,$\pi'_{p-1}$ be the roots of $g$, and let $\pi \in K$ be a root of $f$. Let $\pi'_i$ be the root of $g$ closest to $\pi$, so that $v(\pi - \pi'_i) \geq v(\pi - \pi'_j)$. Then

$$(\pi-\pi'_0)(\pi-\pi'_1)\cdots(\pi-\pi'_{p-1}) = g(\pi) = g(\pi)-f(\pi) = (\omega'-\omega)p\pi^\lambda - \sum_{i\neq\lambda} a_i\pi^i - p(1-a)$$

The valuation of $(\omega'-\omega)p\pi^\lambda$ is greater than 2, since $v(\omega'-\omega) \geq 1$, $v(p) = 1$, $v(\pi^\lambda) > 0$. The valuation of $\sum_{i\neq\lambda} a_i\pi^i$ is at least $1 + \frac{\lambda+1}{p}$, since for $i < \lambda$ we have $v(a_i) \geq 2$, and for $i > \lambda$ we have $v(a_i\pi^i) \geq 1 = \frac{i}{p}$. We have $1 + \frac{\lambda+1}{p} > 1 + \frac{\lambda\frac{p}{p-1}}{p} = 1 + \frac{\lambda}{p-1}$. Finally, $v(p(1-a)) = 1 + v(1-a) \geq 2 > 1 + \frac{\lambda}{p-1}$. Thus

$$v((\pi-\pi'_0)(\pi-\pi'_1)\cdots(\pi-\pi'_{p-1})) > 1 + \frac{\lambda}{p-1}$$

so

$$v(\pi-\pi'_i) > \frac{1+\frac{\lambda}{p-1}}{p} = \frac{1}{p} + \frac{C}{p(p-1)} = v(\pi'_i - \pi'_j)$$

$g$ is Eisenstein and thus irreducible over $\mathbb{Q}_p$, so by Krasner's Lemma $g$ has a root in $K$, and thus $g$ generates $K$.

If we have $\lambda = p-1$, let $1+a'p$ congruent to $a$ mod $p^2$, $g(x) = x^p - \omega' p x^{p-1} - p(1+a'p)$, other notation as before. Then we have

$$(\pi-\pi'_0)(\pi-\pi'_1)\cdots(\pi-\pi'_{p-1}) = g(\pi) = g(\pi) - f(\pi) =$$

$$= (\omega'-\omega)p\pi^{p-1} - \sum_{i<\lambda} a_i\pi^i - p(1+a'p-a)$$

$v((\omega'-\omega)p\pi^{p-1}) \geq 2 + \frac{p-1}{p} > 2$, so the first term has valuation greater than 2. The $a_i$ have valuation at least 2, so the summation has valuation greater than 2. Finally, $v(p(1+a'p-a) = 1 + v(1+a'p-a) \geq 3$, so the last term has valuation greater than two. Then

$$v((\pi-\pi'_0)(\pi-\pi'_1)\cdots(\pi-\pi'_{p-1})) > 2 = 1 + \frac{\lambda}{p-1}$$

so

$$v(\pi-\pi'_i) > \frac{1+\frac{\lambda}{p-1}}{p} = \frac{1}{p} + \frac{C}{p(p-1)} = v(\pi'_i - \pi'_j)$$

so again $g$ generates $K$.

For an extension with case 2, let $\pi$ generate the extension $K$. We need to eliminate the linear term of the minimal polynomial of $\pi$. Let $\alpha = \frac{1}{\frac{1}{\pi} + \frac{a_1}{pa_0}} =$

$\frac{\pi}{1+\pi\frac{a_1}{pa_0}}$, where $a_1$ is the linear and $a_0$ the constant term of the minimal polynomial of $\pi$. Then the minimal polynomial of $\alpha$ has no linear term, $v(\alpha) = \frac{1}{p}$, and $\alpha \equiv \pi$. In terms of operations on the coefficients, the definition of $\alpha$ represents reversing the order (by taking $\frac{1}{\pi}$), eliminating the $x^{p-1}$ term (adding $\frac{a_1}{pa_0}$), and then reversing the order again. Then we can let $f(x)$ be the minimal polynomial of $\alpha$ with coefficients as in previous cases. Let $1 + a'p$ congruent to $a \bmod p^2$, $g(x) = x^p - p(1 + ap)$, other notation as before. Then

$$(\alpha - \pi'_0)(\alpha - \pi'_1)\cdots(\alpha - \pi'_{p-1}) = g(\alpha) = g(\alpha) - f(\alpha) = \sum_{i=2}^{p-1} a_i\alpha^i - p(1 + a'p - a)$$

We have $v(a_i\alpha^i) = v(a_i) + iv(\alpha) \geq 2 + \frac{i}{p} \geq 2 + \frac{2}{p}$, where $v(a_i) \geq 2$ comes from the fact that $f$ is a case 2 Eisenstein polynomial. We have $v(p(1 + a'p - a)) = 1 + v(1 + a'p - a) \geq 3 > 2 + \frac{2}{p}$. Then

$$v((\alpha - \pi'_0)(\alpha - \pi'_1)\cdots(\alpha - \pi'_{p-1})) \geq 2 + \frac{2}{p} = 1 + \frac{p+2}{p} > 1 + \frac{p}{p-1} = 1 + \frac{C}{p-1}$$

so

$$v(\alpha - \pi'_i) > \frac{1 + \frac{C}{p-1}}{p} = \frac{1}{p} + \frac{C}{p(p-1)} = v(\pi'_i - \pi'_j)$$

so again $g$ generates $K$.

Thus the first part of the theorem - existence of roots - is proved. What remains is to show that the first and third classes of polynomials produce distinct extensions. For class 1, this is easy: each of these polynomials has a different value of $\lambda$ or of $\omega \pmod p$. Since we have shown that $\lambda$ and $\omega \pmod p$ are invariants of an extension, adjoining roots of these polynomials must produce distinct extensions. We have the following result:

**Lemma 5.** *$f(x) = x^p - pa$ and $g(x) = x^p - pb$ generate the same extension iff there is $u \in \mathbb{Q}_p$ such that $b = au^p$.*

*Proof.* If $f(x)$ and $g(x)$ generate the same extension, there are $\pi$ and $\pi'$ in $K$ with $f(\pi) = 0$, $f(\pi') = 0$. Let $\pi' = \pi(1+Y)$, $v(Y) > 0$. Then $(1+Y)^p = (\frac{\pi'}{\pi})^p = \frac{b}{a}$. If $Y \notin \mathbb{Q}_p$, then $(1+Y)^p - \frac{b}{a}$ is the minimal polynomial of $Y$. The coefficient of $Y$ in this polynomial is $p$, so by Lemma 3, $1 = v(p) \geq \frac{C}{p} + (p-1)v(Y) = 1 + (p-1)v(Y)$, so $v(Y) \leq 0$, a contradiction. Thus $Y \in \mathbb{Q}_p$, $b = (1+Y)^p a$. Conversely, if $b = au^p$, then if $\pi$ is a root of $x^p - pa$ then $u\pi$ is a root of $g(x)$, so $f(x)$ and $g(x)$ generate the same extension. □

We have the following result:
$u \equiv 1$ in $\mathbb{Q}_p$ (for odd $p$) is a $p$th power iff it is 1 mod $p^2$.

*Proof.* Suppose $k^p = u$. Then $u = k^p \equiv k \pmod p$, so $k \equiv 1$. Let $k = 1 + ap$. Then $u = k^p = 1 + p(ap) + \binom{p}{2}(ap)^2 + ... \equiv 1 \pmod p^2$, so $u$ is 1 mod $p^2$. Now suppose $u$ is 1 mod $p^2$. Then let $u = 1+ap^2$. Let $f(x) = x^p - u$. With $k = 1+ap$,

we have $f(k) = 1 + p(ap) + \binom{p}{2}(ap)^2 + ... - 1 - ap^2 = \binom{p}{2}(ap)^2 + \binom{p}{3}(ap)^3 + ... \equiv 0 \pmod{()p^3}$, so $v(f(k)) \geq 3 > 2 = 2v(pk^{p-1}) = 2v(f'(k))$, so $f$ has a root by Hensel's lemma, and thus $u$ is a $p$th power. (the reason this does not work for $p = 2$ is that the $\binom{p}{2}(ap)^2$ term is not divisible by $p^3$) □

Since $\frac{a}{b} \equiv 1 \pmod{p}^2$ iff $a \equiv b \pmod{p}^2$ for $a$, $b$ congruent to 1, we have that $x^p - pa$ and $x^p - pb$ generate the same extension iff $a$ and $b$ are congruent mod $p^2$. Then we have that the polynomials $x^p - p(1 + ap)$ for $0 \leq a \leq p - 1$ each generate a distinct degree $p$ extension of $\mathbb{Q}_p$, and all extensions with case 2 are generated by these polynomials. Then the proof of the theorem is complete.

The case that was not fully treated by this paper is the second class of polynomials. If $\omega \neq 1$, then $a$ is not necessary, and all extensions are generated by $x^p - \omega x^{p-1} - p$. If $\omega = 1$ then all values of $a$ produce distinct extensions. Proofs of this can (I think) be found in Amano's paper, although the notation involved is somewhat complicated.

Counting the number of polynomials of each class, we have $(p - 1)(p - 2)$ in class 1, $(p - 2) + (p)$ in class 2, and $p$ in class 3, for a total of $p^2$ ramified extensions of $\mathbb{Q}_p$ of degree $p$.

The Galois groups of each of these extensions can be computed. For a table of the canonical polynomials with their parameters along with their Galois groups and inertia groups, see table 2.1 of the paper describing the local fields database.

# References


[1] Amano, S., 1971. Eisenstein equations of degree $p$ in a $\mathfrak{p}$-adic field. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 18, 1–21.

[2] Jones, J. W., & Roberts, D. P. (2003). A database of local fields. arXiv preprint math/0309309.