WILDLY RAMIFIED EXTENSIONS OF $\mathbb{Q}_p$

DRAFT - ARJUN

1. Wildly Ramified Extensions

In review, an extension of Q_p is *ramified* if its set of absolute values is strictly larger than the set of absolute values in Q_p; Ramified extensions have elements with new absolute values, while unramified extensions do not. Some ramified extensions increase the size of the absolute value set more than others. To measure how ramified an extension is, we look at the largest absolute value less than 1. For an algebraic extension, this value can be written as $p^{-\frac{1}{e}}$. We call e the *ramification index* of the extension.

Ramified extensions can further be subdivided into tamely and wildly ramified extension. In *tamely ramified* extensions, e does not divide p, while in *wildly ramified* extensions of e divides p. Wildly ramified extensions are much more numerous than other tamely ramified extensions, and are also extremely hard to categorize outside of certain basic subcases.

The ramification index e cannot be larger than the degree n of the extension, as the it would only contain up to nth roots. Because of this, we call an extension *totally ramified* if $e = n$.

2. Finding extensions

The natural question to ask is whether it is possible to identify and categorize all extensions of $\mathbb{Q}_p$ To answer this, we first look at the general method of finding extensions of $\mathbb{Q}_p$ with degree n, beginning with the following lemma:

Lemma 2.1. *All extensions of $\mathbb{Q}_p$ can be written as a tower of two extensions such that the first is unramified and the second is totally ramified.*

As a result of this lemma, we now only have to categorize all unramified extensions and all totally ramified extensions of unramified extensions.

For totally ramified extensions, the result is trivial: there is exactly one unramified extension of $\mathbb{Q}_p$ for each degree.

For totally ramified extensions, we first take the following lemma, discussed in week 6:

Lemma 2.2. *All Eisentein polynomials in $\mathbb{Q}_p$ generate totally ramified extensions.*

This correlation is also true in reverse (Week 6, problem 5):

Lemma 2.3. *All totally ramified extensions of $\mathbb{Q}_p$ (and of its unramified extensions) can be rewritten as extensions generated by Eisenstein polynomials.*

Thus, we now know that the list of all Eisenstein polynomials, together, generate all totally ramified extensions of $\mathbb{Q}_p$. To find a minimal set of extensions, the simplest approach is just to run through the list and exclude polynomials whose roots are in extensions generated by previous polynomials; the issue, however, is that there are an infinite number of Eisenstein

Date: June 12, 2018.

polynomials. The task then becomes finding a *finite* list of Eisenstein polynomials that still generates all totally ramified extensions.

The way we do this is by taking the prime ideal $\mathcal{P}$ of the initial unramified extension $\mathcal{K}$. We can then take the ideal quotient group $\mathcal{P}_l/\mathcal{P}_m$, with $m \geq l$, and take Eisenstein polynomials with coefficients taken from these quotient groups.

We select both l and m based on the desired relative discriminant of the extension, which can be written as $\mathcal{P}^{n+j-1}$. The possible discriminants for extensions are limited and can be found using *Ore's conditions*:

Proposition 2.4. *(Ore's conditions): There exist totally ramified extensions of* $\mathcal{K}$ *with degree* n *and discriminant* $\mathcal{P}^{n+j-1}$ *if and only if*

$$\min\{v_p(b)n, v_p(n)n\} \leq j \leq v_p(n)n$$

Where b *is the remainder of* j *modulo* p*.*

We now have a set of finite j which correspond to degree n extensions. For each j, set $a = \lfloor \frac{j}{p} \rfloor$ and $b = j \mod p$. We can now set m as some integer satisfying
$m > \frac{n+2j}{n}$.

For the quotient from which the ith coefficient is taken, we set

$$l(i) = \begin{cases} \max\{2 + a - v_p(i), 1\} & i < b \\ \max\{1 + a - v_p(i), 1\} & i \geq b \end{cases}$$

We then construct the polynomials with coefficients of the ith degree term taken from $\mathcal{P}_{l(i)}/\mathcal{P}_m$, with the exception of the constant term, which is taken from $\mathcal{P}_1/\mathcal{P}_m$. We also restrict the constant and bth degree terms to only values with p-adic valuation $l(i)$.

The resulting list of polynomials is finite, and can be proven to generate all totally ramified degree n extensions of $\mathcal{K}$ with discriminant $\mathcal{P}^{n+j-1}$.

3. Results for Tamely Ramified Extensions

A formula by Krasner counts the number of totally ramified extensions of $\mathcal{K}$. This further simplifies the search process outlined earlier; we can now search through our new, finite list of Eisenstein polynomials, adding to the final list those with roots not in any extensions generated by any polynomials already added to the final list until the requisite number has been reached. Once this has been done for all j satisfying Ore's conditions, we have our complete results.

In two cases, ramified extensions can be categorized nicely into closed forms. The simpler of the cases is that of tamely ramified extensions:

Theorem 3.1. *The totally and tamely ramified degree* n *extensions of an unramified degree* f *extension* $\mathcal{K}/\mathbb{Q}_p$ *are generated by the roots of the polynomials* $x^n - \zeta^r p$ *where* ζ *is a* (p^f-1)*th root of unity for all* $0 \leq r < p^f - 1$*. Two such extensions are isomorphic only if their values of* r *are equivalent mod* $\gcd(n, p^f - 1)$*.*

This gives us a total of n degree n totally and tamely ramified extensions of $\mathcal{K}$.

4. Degree p extensions with p odd

Degree p extensions are the second case with a closed form, and are much easier to classify than other wildly ramified extensions. For all odd p, each of the following polynomials defines one of the degree p extensions of $\mathbb{Q}_p$:

1. $x^p + (p + ap^2)\ \forall\ 0 \leq a \leq p - 1$
2. $x^p + px^{p-1} + (p + ap^2)\ \forall\ 0 \leq a \leq p - 1$
3. $x^p + ap^\lambda + p\ \forall\ 1 \leq a \leq p - 1, 1 \leq \lambda \leq p - 1, (a, \lambda) \neq (p - 1, p - 1)$

Each of the first two categories define p extensions, and the third defines $p^2 - 2p$ extensions, for a total of p^2 extensions, a dramatically faster increase than the unramified or tamely ramified extensions.

5. Composite Wild Ramification

Unfortunately, composite cases of wild ramification are trickier. They grow much faster; there are already 59 quartic extensions of $\mathbb{Q}_2$. There is currently no closed form for any meaningful grouping of these cases; and such a form is considered unlikely to exist. For each of these cases, the more lengthy process described in Section 2 must be used in full.

Euler Circle, Palo Alto, CA 94306
E-mail address: arjun.b.venkatraman@gmail.com