CHAPTER 3

The number of totally ramified extensions of $\mathbb{Q}_p$ of degree n

3.1. Eisenstien polynomials and totally ramified extensions

For fixed n and j, write $j = an + b$, where $0 \leq b < n$. In this section we will construct a finite set of Eisenstien polynomials of degree n and with polynomials' discriminant belongs to $M_p^{n+j-1} \setminus M_p^{n+j}$ that generate all totally ramified extensions of $\mathbb{Q}_p$ of degree n and with discriminant M_p^{n+j-1}.

For convenience we list two notations in this section:

$K_{n,j}$: the set of all totally ramified extensions of $\mathbb{Q}_p$ of degree n with discriminant M_p^{n+j-1}.

$E_{n,j}$: the set of all Eisenstien polynomials of degree n with discriminant whose valuation is $n + j - 1$ by $E_{n,j}$.

Given an element in $E_{n,j}$, say $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. let α be a root of $f(x)$ and we have

$$\upsilon_p(f'(\alpha)) = \frac{n+j-1}{n} = 1 + a + \frac{b-1}{n}.$$

But $\upsilon_p(f'(\alpha)) = \upsilon_p(n\alpha^{n-1} + \cdots + a_1)$. Since $\upsilon_p(ia_i\alpha^{i-1}) = \upsilon_p(i) + \upsilon_p(a_i) + \frac{i-1}{n}$ are all distinct for $i = 1, \cdots, n$, where we set $a_n = 1$, we have

$$1 + a + \frac{b-1}{n} = \min_{1 \leq i \leq n} \{\upsilon_p(ia_i\alpha^{i-1})_p\} = \upsilon_p(b) + \upsilon_p(a_b) + \frac{b-1}{n}, \text{ if } b \neq 0,$$

$$1 + a + \frac{-1}{n} = \min_{1\le i\le n}\{v_p(ia_i\alpha^{i-1})\} = v_p(n) + v_p(a_n) + \frac{n-1}{n}, \quad \text{if } b = 0.$$

Hence for $i \neq b$, $v_p(i) + v_p(a_i) + \dfrac{i-1}{n} > 1 + a + \dfrac{b-1}{n}$, which implies

$$v_p(a_i) \ge 2 + a - v_p(i), \quad \text{if } i < b,$$

$$v_p(a_i) \ge 1 + a - v_p(i), \quad \text{if } i > b.$$

For $1 \le i \le n$, define

$$h(i) := \begin{cases} \max\{2 + a - v_p(i),\ 1\}, & \text{if } i < b, \\ \max\{1 + a - v_p(i),\ 1\}, & \text{if } i \ge b. \end{cases}$$

Hence for $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in E_{n,j}$, we have

$$v_p(a_i) = 1 \qquad \text{if } i = 0,$$

$$v_p(a_i) \ge h(i) \quad \text{if } 1 \le i \le n-1 \text{ and } i \neq b,$$

$$v_p(a_i) = h(b) \quad \text{if } i = b \neq 0.$$

Recall that for α as a root of $f(x)$,

$$|f'(\alpha)|_p = \prod_{i=2}^{n} |\alpha - \alpha_i|_p \le \min_{2\le i\le n}\{|\alpha - \alpha_i|_p\} p^{-\frac{n-2}{n}},$$

because $|\alpha - \alpha_i| \le p^{-\frac{1}{n}}$ for all i. Since $|f'(\alpha)|_p = p^{-\frac{n+j-1}{n}}$, this implies

$$\min_{2\le i\le n}\{|\alpha - \alpha_i|_p\} \ge p^{-\frac{j+1}{n}}.$$

Now we want to find an integer c such that for $g(x) \in E_{n,j}$ with $|f - g|_p \le p^{-c}$, there is a root β of $g(x)$ satisfying

$$|\beta - \alpha|_p < \min_{2\le i\le n}\{|\alpha - \alpha_i|_p\}.$$

Choose β among the roots of $g(x)$ such that $|\beta - \alpha|_p$ is minimal. To make $|\beta - \alpha|_p < |\alpha - \alpha_i|_p$ for all i, we select $g(x)$ such that $|\beta - \alpha|_p < p^{-\frac{j+1}{n}}$. Then

$$|f-g|_p = \prod_{i=1}^{n} \max\{|\beta-\alpha|_p, |\alpha-\alpha_i|_p\}.$$
$$= |\beta-\alpha|_p |f'(\alpha)|_p < p^{-\frac{n+2j}{n}},$$

Hence we may choose $c > \dfrac{n+2j}{n}$. In the following step we will explain how to find generating polynomials.

Let $k \geq h \geq 1$ be two integers, and $R_{h,k}$ a set of representatives of the quotient M_p^h/M_p^k. We denote the subset of $R_{h,k}$ whose valuation is exactly h by $R_{h,k}^*$.

Let $c = \lfloor \dfrac{n+2j}{n} \rfloor + 1$, where $\lfloor m \rfloor$ means an integer which is maximal in the set of integers less or equal to m. Define $w = (w_0, \cdots, w_{n-1}) \in \mathbb{Q}_p^n$ such that

$$w_i \in \begin{cases} R_{1,c}^* & \text{if } i = 0, \\ R_{h(i),c} & \text{if } 1 \leq i \leq n-1 \text{ and } i \neq b, \\ R_{h(b),c}^* & \text{if } i = b \neq 0. \end{cases}$$

Let Ω denote the set of all $w \in \mathbb{Q}_p^n$ satisfying above conditions. For each $w \in \Omega$, we associate the polynomial $f_w(x) := x^n + w_{n-1}x^{n-1} + \cdots + w_0$. For $w \in \Omega$, let $D_{E_{n,j}}(f_w,\ r) := \{f(x) \in E_{n,j}\ ; |f - f_w|_p \leq r\}$. Then we have the following results.

LEMMA 3.1.1. *Let $c = \lfloor \dfrac{n+2j}{n} \rfloor + 1$. Then the polynomial $f_w(x)$ is an Eisenstien polynomial with discriminant M_p^{n+j-1} for all $w \in \Omega$. Let w, w' be two distinct elements in Ω, then $D_{E_{n,j}}(f_w,\ r)$ and $D_{E_{n,j}}(f_{w'},\ r)$ are disjoint. Furthermore, the set $E_{n,j}$ is the disjoint union of the closed discs $D_{E_{n,j}}(f_w,\ r)$, where $r = p^{-c}$.*

Proof. See [**5**, p.1646]. □

COROLLARY 3.1.2. *Every totally ramified extension of $\mathbb{Q}_p$ of degree n and discriminant M_p^{n+j-1} can be written as $\mathbb{Q}_p(\pi)$, where π is a root of $f_w(x)$ for some $w \in \Omega$.*

Proof. Let K be an element in $K_{n,j}$ and α a prime element of K, $f(x) = \text{Irr}(\alpha, \mathbb{Q}_p)$. Let $\alpha = \alpha_1, \cdots, \alpha_n$ be roots of $f(x)$. Then

$$|f'(\alpha)|_p = \prod_{i=2}^{n} |\alpha - \alpha_i|_p \leq p^{-\frac{n-2}{n}} \min_{2\leq i\leq n}\{|\alpha - \alpha_i|_p\}.$$

But $|f'(\alpha)|_p = p^{-\frac{n+j-1}{n}}$, which implies

$$\min_{2\leq i\leq n}\{|\alpha - \alpha_i|_p\} \geq p^{-\frac{j+1}{n}}.$$

By lemma 3.1.1 there exists f_w for some w such that $|f - f_w|_p \leq r$. Let π be a root of $f_w(x)$ such that $|\pi - \alpha|_p \leq |\pi_i - \alpha|_p$ for all π_i as conjugates of π. If $|\pi - \alpha|_p \geq \min_{2\leq i\leq n}\{|\alpha - \alpha_i|_p\}$, then

$$\begin{aligned} |f - f_w|_p &= \prod_{i=1}^{n} \max\{|\pi - \alpha|_p, |\alpha - \alpha_i|_p\} \\ &\geq \prod_{i=1}^{n} \max\{\min_{2\leq i\leq n}\{|\alpha - \alpha_i|_p\}, |\alpha - \alpha_i|_p\} \\ &= \min_{2\leq i\leq n}\{|\alpha - \alpha_i|_p\} |f'(\alpha)|_p \geq p^{-\frac{n+2j}{n}} > p^{-c}, \end{aligned}$$

contradiction. □

3.2. Calculate the number of totally ramified extensions of $\mathbb{Q}_p$

In this section we will give a formula to calculate the number of totally ramified extensions of $\mathbb{Q}_p$ of degree n.

Even if the distance of two Eisenstein polynomials is not sufficient small, they may generate the same field extension. In the next theorem, we will discuss the relation between the number of generating polynomials in $E_{n,j}$ and of elements in $K_{n,j}$.

THEOREM 3.2.1. *Let $t = nc - n - j + 1$ and $r = p^{-c}$, where $c = \lfloor \frac{n+2j}{n} \rfloor + 1$. Let $\aleph(D_{E_{n,j}}(r))$ denote the number of disjoint closed discs of radius r. Then the number of elements in $K_{n,j}$ is $\aleph(D_{E_{n,j}}(r)) \frac{n}{(p-1)p^{t-2}}$.*

Proof. Let $\Pi_{n,j}$ denote the set of all prime elements in $K_{n,j}$. In fact, $\Pi_{n,j}$ is the union of $M_K \backslash M_K^2$, where K runs through elements in $K_{n,j}$. Define the map $\varphi : \Pi_{n,j} \to E_{n,j}$ by $\varphi(\alpha) = \mathrm{Irr}(\alpha, \mathbb{Q}_p)$. Now we want to claim that $D_{E_{n,j}}(\varphi(\alpha), r) = \varphi(D(\alpha, p^{-\frac{t}{n}}))$ for all $\alpha \in \Pi_{n,j}$. For $\beta \in D(\alpha, p^{-\frac{t}{n}})$, $|\beta - \alpha|_p \leq p^{-\frac{t}{n}} < p^{-\frac{j+1}{n}} \leq \min_{2 \leq i \leq n}\{|\alpha - \alpha_i|_p\}$. If $|\beta - \alpha_i|_p > |\alpha - \alpha_i|_p$ for some i, $|\beta - \alpha|_p = |\beta - \alpha_i|_p$, contradicts with $|\beta - \alpha|_p < \min_{2 \leq i \leq n}\{|\alpha - \alpha_i|_p\}$

$$|\varphi(\beta) - \varphi(\alpha)|_p = |\beta - \alpha|_p \prod_{i=2}^{n} |\beta - \alpha_i|_p$$

$$\leq p^{-\frac{t}{n}} \prod_{i=2}^{n} |\alpha - \alpha_i|_p$$

$$= p^{-\frac{t}{n}} p^{-\frac{n+j-1}{n}} = p^{-c} = r.$$

Conversely, For $f(x) \in D_{E_{n,j}}(\varphi(\alpha), r)$, let β be a root of $f(x)$ such that $|\beta-\alpha|_p$ is minimal among conjugates of β. If $|\beta - \alpha|_p > p^{-\frac{t}{n}}$, then by lemma 2.4.3,

$$|f - \varphi(\alpha)|_p = \prod_{i=1}^{n} \max\{|\beta - \alpha|_p, |\alpha - \alpha_i|_p\}$$

$$> \prod_{i=1}^{n} \max\{p^{-\frac{t}{n}}, |\alpha - \alpha_i|_p\}$$

$$= p^{-\frac{t}{n}} \prod_{i=2}^{n} |\alpha - \alpha_i|_p = p^{-c},$$

contradiction. Hence $\beta \in D(\alpha, p^{-\frac{t}{n}})$. Now, the map φ is surjective and one-to-one. Furthermore, because $\min\{|\alpha_i - \alpha_j|_p\} > p^{-\frac{t}{n}}$, $\{D(\alpha_i, p^{-\frac{t}{n}})\}$ are all disjoint where α_i are conjugates of α. We conclude that the inverse image of any closed disc of radius r in $E_{n,j}$ is the disjoint union of n closed discs of radius $p^{-\frac{t}{n}}$ in $\Pi_{n,j}$. But by lemma 2.4.1, if $\beta \in D(\alpha, p^{-\frac{t}{n}})$, $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$, hence any such disc is in fact contained in $M_K \backslash M_K^2$ for some $K \in K_{n,j}$ and the number of disjoint discs of radius $p^{-\frac{t}{n}}$ in M_K is the number of $R_{1,t}^*$, which equals $p^{t-1} - p^{t-2}$, and so $\aleph(K_{n,j})p^{t-2}(p-1) = n\aleph(D_{E_{n,j}}(r))$. $\square$

REMARK 2. For fixed n and j which satisfies *Ore's condition* with respect to n, let $t = nc - n - j + 1$ and $r = p^{-c}$, where $c = \lfloor \frac{n+2j}{n} \rfloor + 1$. For fixed an element K in $K_{n,j}$, let R_K be the representatives of prime elements of K modulo M_K^t. Define a map $\tilde{\varphi}$ from $\Pi_{n,j}$ to Ω by $\tilde{\varphi}(\alpha) = w$, where w is the unique element satisfying $\varphi(\alpha) \in D_{En,j}(f_w, r)$. Then in the proof of theorem 3.2.1 we know that the set $\{\tilde{\varphi}(\beta); \beta \in R_K\}$ is exactly the set of $w \in \Omega$ such that K and any root of f_w defines a $\mathbb{Q}_p-$isomorphic extension. This

conclusion can help us to classify totally ramified extensions of $\mathbb{Q}_p$ of degree n with discriminant M_p^{n+j-1} to $\mathbb{Q}_p-$isomorphic extensions.

In fact, we can calculate $\aleph(D_{E_{n,j}}(r))$:

PROPOSITION 3.2.2. *Note that $r = p^{-c}$. Then*

$$\aleph(D_{E_{n,j}}(r)) = \begin{cases} (p-1)p^{nc-n-j-1+\sum_{i=1}^{a}\frac{n}{p^i}} & \text{if } b = 0, \\ (p-1)^2 p^{nc-n-j-1+\sum_{i=1}^{a}\frac{n}{p^i}+\frac{b-1}{p^{a+1}}} & \text{if } b > 0. \end{cases}$$

Proof. See[**5**, p.1648]. □

Example Let $n = 2$. By remark 1 we classify this example to p :

(1) $p \neq 2$. Then j must be equal to 0 and all totally ramified extensions of $\mathbb{Q}_p$ of degree 2 have the same discriminant M_p. In this case we have $c = 2$, $t = 3$, and $j = 0 \cdot n + 0$ and hence we can calculate the number of elements in $K_{2,0}$:

$$\aleph(K_{2,0}) = \frac{2}{(p-1)p}\aleph(D_{E_{2,0}}(p^{-2})) = \frac{2}{(p-1)p}(p-1)p = 2.$$

Hence we conclude that there are only two totally ramified extensions of $\mathbb{Q}_p$ of degree 2 in the case $p \neq 2$.

(2) $p = 2$. By proposition 2.5.6 we have j may be 1 or 2. We calculate the number separately.

(i) $j = 1$. We write $j = 0 \cdot 2 + 1$. Then we have $c = 3$ and $t = 4$. Hence we can calculate the number of elements in $K_{2,1}$:

$$\aleph(K_{2,1}) = \frac{2}{2^2}\aleph(D_{E_{2,1}}(2^{-3})) = \frac{1}{2}2^2 = 2.$$

(ii) $j = 2$. We write $j = 1 \cdot 2 + 0$. Then we have $c = 4$ and $t = 5$. Hence we can calculate the number of elements in $K_{2,2}$:

$$\aleph(K_{2,2}) = \frac{2}{2^3}\aleph(D_{E_{2,2}}(2^{-4})) = \frac{1}{4}2^4 = 4.$$

Hence we conclude that there are six totally ramified extensions of $\mathbb{Q}_2$ of degree 2. $\square$