Contents

1 Lecture 1 (Malcolm Kotok - September 5, 2012) 2
   1.1 Introduction ......................................................... 2
   1.2 $p$-adic fields ......................................................... 2
       1.2.1 Representation of $\mathbb{Q}_p$ ................................. 3
   1.3 Algebraic Extensions of $\mathbb{Q}_p$ ................................. 4

2 Lecture 2 (Meg Walters - September 10, 2012) 4

3 Lecture 3 (Dillon Ethier) 6

4 Lecture 4 - Brendan Murphy 8

5 Extensions of $\mathbb{Q}_p$ 8
   5.1 Teichmüller Digits .................................................. 8
   5.2 The completion of $\overline{\mathbb{Q}}_p$ ............................... 9

6 $p$-adic Power Series 9
   6.1 The $p$-adic Exponential and Logarithm ................................ 10
   6.2 Newton Polygons ..................................................... 11

7 Lecture 5 - Siegfred 13

8 Lecture 6 - Jamie 16

9 Lecture 7 - Malcolm 18
   9.1 $L$-functions ....................................................... 18

10 Lecture 8 - Meg 19

11 Lecture 9 - Dillon 22

12 Lecture 10 - Brendan 23
   12.1 The Newton Polygon of $\det(1 - \alpha_a T)$ .......................... 23
   12.2 $p$-adic Directness ................................................ 24
   12.3 Side Note ............................................................ 25

13 Lecture 11 - Siegfred 25

14 Lecture 12 - Jamie 28

15 Lecture 13 - Malcolm 31
   15.1 Ehrart Theory ....................................................... 31

16 Lecture 14 - Meg 33

17 Lecture 15 - Dillon 35
1.1 Introduction

$L$-functions of (toric) exponential sums over finite fields. Let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ and for each $m \in \mathbb{Z}_{\geq 1}$ define:

$$S_m = \sum_{x_1, \ldots, x_n \in \mathbb{F}_q^*} \exp \left( \frac{2\pi i}{p} \cdot \text{Tr}_{\mathbb{F}_q/m/\mathbb{F}_p}(f(x_1, \ldots, x_n)) \right) \in \mathbb{C}$$

- $p$-adic approach: “more analytic in nature”
- $\ell$-adic approach ($\ell \neq p$, $\ell$ prime): “rep. theory more algebraic in nature”

Definition 1.1.

$$L(f, t) := \exp \left( \sum_{m=1}^{\infty} S_m \frac{T_m}{m} \right)$$

Theorem 1.2.

$$L(f, t) = \frac{\prod_{i=1}^{M}(1 - \alpha_i T)}{\prod_{j=1}^{N}(1 - \beta_j T)} \iff S_m = \sum_{j=1}^{M} \beta_j^m - \sum_{i=1}^{M} \alpha_i^m \quad \forall m.$$
Theorem 1.5. $| \cdot |_p$ satisfies the following:

1. $|a|_p \geq 0 \quad |a| = 0 \iff a = 0$.
2. $|ab|_p = |a| \cdot |b|$
3. $|a + b| \leq \max\{|a|, |b|\} \leq |a| + |b|$ (Ultrametric norm)

To obtain $\mathbb{Q}_p$ we complete $\mathbb{Q}$ via Cauchy sequences with the norm $| \cdot |_p$, just like we obtain $\mathbb{R}$ when we complete $\mathbb{Q}$ via Cauchy sequences with the usual norm $| \cdot |$.

Proposition 1.6.

\[
\sum_{i=0}^{\infty} a_i \text{ converges in } \mathbb{Q}_p \iff \lim_{i \to \infty} a_i = 0
\]

Proof.

$(\Rightarrow)$ Same as in $\mathbb{R}$.
$(\Leftarrow)$ Let $S_n := \sum_{i=0}^{N} a_i$. We will show that $\{S_N\}$ is Cauchy.

\[
|S_N - S_M| = \left| \sum_{i=M+1}^{N} a_i \right| \leq \max_{i=M+1}^{N} |a_i| < \epsilon \quad M \gg 0
\]

$\square$

1.2.1 Representation of $\mathbb{Q}_p$

\[
\mathbb{R} : \sum_{i=-\infty}^{\infty} b_i 10^{-i}, \quad 0 \leq b_i \leq 9
\]

\[
\mathbb{Q}_p : \sum_{i=-\infty}^{\infty} b_i p^i, \quad 0 \leq b_i \leq p - 1
\]

For example if $p = 3$ then one representation could be $1 + 3 + 2 \cdot 3^2 + 3^3 + \cdots \in \mathbb{Q}_3$.

Definition 1.7.

\[
\mathbb{Z}_p := \{a \in \mathbb{Q}_p : |a|_p \leq 1\}
\]

Theorem 1.8. Every equivalence class $\alpha \in \mathbb{Z}_p$ has exactly one representative $\{a_i\}_{i=0}^{\infty}$ such that

1. $0 \leq a_i \leq p^{i+1}, \; i = 0, 1, 2, \ldots$
2. $a_i \equiv a_{i+1} \mod (p^i), \; i = 0, 1, 2, \ldots$

Proof. [Kob, Thm 2, I.4]

This means if $\alpha \in \mathbb{Z}_p$ then for $0 \leq b_i \leq p - 1$ we have,

\[
\alpha = b_0 + b_1 p + b_2 p + \cdots
\]

Next for $\alpha \in \mathbb{Q}_p$, then there is an $N$ such that $p^N \alpha \in \mathbb{Z}_p$

\[
|p^N \alpha| = \frac{1}{p^N} |\alpha| \xrightarrow{(N \gg 0)} p^N \alpha \in \mathbb{Z}_p.
\]

$\Rightarrow$ $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. 

3
Definition 1.9. If \( \alpha = b_n p^n + b_{n+1} p^{n+1} + \cdots = p^n (b_n + b_{n+1} p + \cdots) \), then

\[
\text{ord}_p(\alpha) = n \quad \text{and} \quad |\alpha|_p = \frac{1}{p^n}
\]

Definition 1.10.
\[
p\mathbb{Z}_p := \{ a \in \mathbb{Q}_p : |a| < 1 \} = \{ a \in \mathbb{Z}_p : |a| < 1 \}
\]

Notes: [Kob, Chap III]
1. \( \mathbb{Z}_p \) is a ring
2. \( p\mathbb{Z}_p \) is a maximal ideal in \( \mathbb{Z}_p \)
3. \( \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p = \{0, 1, \ldots, p - 1\} \)

1.3 Algebraic Extensions of \( \mathbb{Q}_p \)
Let \( f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \) (\( a_i \in \mathbb{Q}_p \)) be irreducible over \( \mathbb{Q}_p \). Let \( \alpha \) be a root and define

\[
K := \mathbb{Q}_p(\alpha) = \{ b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1} \mid b_i \in \mathbb{Q}_p \}.
\]

Clearly \( \mathbb{Q}_p \to K \) by \( a \mapsto a + 0\alpha + \cdots + 0\alpha^{n-1} \) and thus \( \mathbb{Q}_p \leq K \). \( \mathbb{Q}_p \) has norm \( |\cdot|_p \), but how do we extend this to \( K \)?

Definition 1.11. (Algebraic) norm of an element:
1. \( N_{K/\mathbb{Q}_p}(\alpha) := (-1)^n a_0 \).
2. \( N_{K/\mathbb{Q}_p}(\alpha) := \alpha_1 \alpha_2 \cdots \alpha_n \), where \( \alpha_i \) are the conjugate roots of \( \alpha = \alpha_1 \).
3. Define a linear map \( T_\alpha : K \to K \) by multiplication by \( \alpha \). i.e. \( T_\alpha(a) = \alpha a \). \( N_{K/\mathbb{Q}_p}(\alpha) := \det(T_\alpha) \).

To guess at a definition of the extension look at \( \mathbb{Q}_p \rightarrow K \) by \( a \mapsto a + 0\alpha + \cdots + 0\alpha^{n-1} \) and thus \( \mathbb{Q}_p \leq K \). \( \mathbb{Q}_p \) has norm \( |\cdot|_p \), but how do we extend this to \( K \)?

Fact: Extensions of \( |\cdot|_p \) on \( \mathbb{Q}_p \) are unique. i.e. \( \forall \beta \in K, |\beta| = |\beta|' \). We know \( N_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p \), thus

\[
|N_{K/\mathbb{Q}_p}(\alpha)|_p = ||N_{K/\mathbb{Q}_p}(\alpha)|| = ||\alpha_1 \cdot \alpha_2 \cdots \alpha_n|| = ||\alpha||^n \implies ||\alpha|| = |N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n}
\]

2 Lecture 2 (Meg Walters - September 10, 2012)
Recall from last time that we have a norm

\[
|\cdot|_p : \mathbb{Q} \to \mathbb{Q}_p
\]
In addition, we have \( \mathbb{Z}_p \subseteq \mathbb{Q}_p \), where

\[
\mathbb{Z}_p = \{ a \in \mathbb{Q}_p : |a| \leq 1 \}
\]

For \( K \) such that \( [K : \mathbb{Q}_p] < \infty \), we would like to extend this norm to \( K \).

Definition. For \( \alpha \in K \), define the norm

\[
||\alpha|| := |N_{K/\mathbb{Q}_p}(\alpha)|^{1/[K:\mathbb{Q}_p]}
\]

where

\[
N_{K/\mathbb{Q}_p}(\alpha) := N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)^{[K:\mathbb{Q}_p(\alpha)]}
\]

Proposition. Indeed, \( |\cdot| \) extends \( |\cdot|_p \) and is a norm. (Extension is unique)

Notation. For \( \alpha \in K \), define

\[
\text{ord}_p(\alpha) := -\log_p |\alpha|
\]

\[
= -\frac{1}{[\alpha : \mathbb{Q}_p]} \log |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p
\]

\[
= \frac{\text{ord}_p \left( |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p \right)}{[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]} \in \frac{1}{[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]} \mathbb{Z}
\]

As a side note, recall that if \( a \in \mathbb{Q}_p \), then

\[
|a|_p = \frac{1}{p^\text{ord}_p(a)}
\]

and \( \text{ord}_p(a) \) is a valuation.
Structure of p-adic fields

Proposition. Let \([K : \mathbb{Q}_p] = n < \infty\). Let \(A := \{\alpha \in K : |\alpha| \leq 1\}\) and \(M := \{\alpha \in K : |\alpha| < 1\}\) (recall that previously we saw an example where \(A = \mathbb{Z}_p\) and \(M = p\mathbb{Z}_p\)). Then:

1) \(A\) is a ring, \(M\) is an ideal.
2) \(A\) is the integral closure of \(\mathbb{Z}_p\) in \(K\). (Meaning \(A = \{\alpha \in K : \alpha\) is a root of a monic polynomial over \(\mathbb{Z}_p\) \).
3) \(M\) is the unique maximal ideal of \(A\) (hence \(A\) is a local ring).
4) \([A/M : \mathbb{F}_p] \leq [K : \mathbb{Q}_p]\)

Proof of 1). Let \(\alpha, \beta \in A\). Then

\[|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\} \leq 1\]

and

\[|\alpha \beta| = |\alpha||\beta| \leq 1\]

This implies that \(\alpha \beta, \alpha + \beta \in A\). The proof is similar for \(M\) an ideal. The details are left as an exercise. \(\square\)

Proof of 2). Let \(\alpha \in K\) be integral over \(\mathbb{Z}_p\). Thus, \(\alpha\) satisfies

\[x^m + a_{m-1}x^{m-1} + \cdots + a_0\]

where \(a_i \in \mathbb{Z}_p\). We need to show that \(|\alpha|_p \leq 1\).

Suppose not, so \(|\alpha| > 1\). Then we have

\[|\alpha|^m = |\alpha|^m\]
\[= |a_{m-1}\alpha^{m-1} - \cdots - a_0|\]
\[\leq \max_{i=1,2,\ldots,m} \{a_{m-i}\alpha^{m-i}\}\]
\[\leq \max_{i=1,2,\ldots,m} \{|\alpha|^{m-i}\} = |\alpha|^{m-1}\]

since \(|\alpha|^{m-i}\) is biggest when \(i = 1\). This is a contradiction since \(|\alpha| > 1\), proving that the integral closure is contained in \(A\).

Now for the proof in the other direction. Let \(\alpha \in A\) and so \(|\alpha| \leq 1\). From last time, we know that all Galois conjugates over \(\mathbb{Q}_p\) of \(\alpha\) have the same norm. Let \(\alpha_1, \ldots, \alpha_m\) be the conjugates of \(\alpha\). Consider

\[f(x) = (x - \alpha_1)\cdots(x - \alpha_m) \in \mathbb{Q}_p[x]\]

Multiplying out we get

\[f(x) = x^m - (\alpha_1 + \cdots + \alpha_m)x^{m-1} + \left(\sum \alpha_i\alpha_j\right)x^{m-2} + \cdots + (-1)^m\alpha_1\cdots\alpha_m\]

Notice the coefficients of this equation are actually in \(\mathbb{Z}_p\). For example,

\[|\alpha_1 + \cdots + \alpha_m| \leq \max\{|\alpha_i|\} \leq 1\]

which implies that \(\alpha_1 + \cdots + \alpha_m \in \mathbb{Z}_p\). The argument is similar for the rest of the coefficients. This implies that \(A\) is contained in the integral closure of \(\mathbb{Z}_p\) in \(K\). \(\square\)

Proof of 3). Let \(I \subseteq A\) be an ideal. Suppose that there exists \(\alpha \in I\setminus M\). Then \(|\alpha| = 1\), which implies that \(|\frac{1}{\alpha}| = 1\), so \(\frac{1}{\alpha} \in A\). From this, we have \(1 \in \frac{1}{\alpha}I \subseteq I\). This implies that \(I = A\), which is a contradiction. \(\square\)

Proof of 4). Since \(M\) is a maximal ideal, \(A/M\) is a field. Next, we will show that \(\text{char}(A/M) = p\). Note that \(\mathbb{Z}_p \rightarrow A\) and \(M \cap \mathbb{Z}_p = p\mathbb{Z}_p\). This gives us a map

\[\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p \rightarrow A/M\]

with \(a + p\mathbb{Z}_p \mapsto a + M\). This map is a field homomorphism and so it is injective, proving that \(\text{char}(A/M) = p\).

Next we will prove the degree estimate. Let \([K : \mathbb{Q}_p] = n\). Let \(\overline{a_1}, \ldots, a_{n+1} \in A/M\). We will show that these are linearly dependent over \(\mathbb{F}_p\). Lift \(\overline{a_1}, \ldots, a_{n+1} \) to \(a_1, \ldots, a_{n+1} \in A\) such that \(a_i \equiv \overline{a_i}\) mod \(M\). Then there exist \(b_i \in \mathbb{Q}_p\), not all zero, such that

\[b_1a_1 + \cdots + b_{n+1}a_{n+1} = 0\]

Multiply this equation by \(p^r\) for some \(r\) such that

1) \(p^rb_i \in \mathbb{Z}_p\) for each \(i\)
2) \((p^rb_i) \in \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p \neq 0\) for some \(i\).

Then

\[(p^rb_1)a_1 + \cdots + (p^rb_{n+1})a_{n+1} = 0\]

in \(A/M\). By construction, not all of the coefficients are zero, so \(\overline{a_1}, \ldots, a_{n+1} \) are linearly dependent over \(\mathbb{F}_p\). \(\square\)
Definition. $A/M$ is called the residue field of $K/Q_p$.

We saw for $\alpha \in K$,

\[
\text{ord}_p(\alpha) \in \frac{1}{[K : Q_p]} \mathbb{Z}
\]

which is a group under addition. Since $|\alpha \beta| = |\alpha| \cdot |\beta|$ if and only if $\text{ord}_p(\alpha \beta) = \text{ord}_p(\alpha) + \text{ord}_p(\beta)$, the map

\[
\text{ord}_p : (K\{0\}, \cdot) \to \frac{1}{[K : Q_p]} \mathbb{Z}
\]

is a group homomorphism.

As an exercise, show that $\text{Im}(\text{ord}_p) = \frac{1}{e} \mathbb{Z}$ for some $e \geq 1$ with $e | [K : Q_p]$.

$e$ is called the ramification index of $K/Q_p$. If $e = 1$, we say that $K$ is unramified. If $e = [K : Q_p]$, we say $K$ is totally ramified. (If $p | e$ we say wild ramification and if $e \nmid p$ we say tame ramification.)

Uniformizer: Let $\pi \in K$ such that $\text{ord}_p(\pi) = \frac{1}{e}$. Then, for all $\alpha \in K$, there exists $u \in A$ and $m \in \mathbb{Z}$ such that $\alpha = u \pi^m$, where $|u| = 1$.

As an exercise, show that $M = (\pi)$.

Recall that we have the following diagram, where $n$ and $f$ represent the indices $[K : Q_p]$ and $[A/M : F_p]$, respectively. We know that $f \leq n$, $\text{ord}_p(\pi) = \frac{1}{e}$, where $e$ is the ramification index.

```
\begin{array}{ccc}
K & A/M \\
\downarrow{n} & \downarrow{f} \\
Q_p & F_p
\end{array}
```

Proposition. $n = ef$

Proof. We know that $A/M \cong F_p$. Let $\overline{w}_1, \ldots, \overline{w}_f$ be a basis of $A/M$ over $F_p$. Let $w_1, \ldots, w_f \in A/M$ such that $w_i = \overline{w}_i \text{mod}(M)$.

Claim:

\[
\{w_i \pi^j | 1 \leq i \leq f, 0 \leq j \leq e - 1\}
\]

is a basis for $K$ over $Q_p$.

First we will prove that this set spans $K$ over $Q_p$. Take an arbitrary $\alpha \in K$. Without loss of generality, we can assume that $\alpha \in A$. Let $\overline{\alpha}$ be a corresponding element in $A/M$. Then there exist $b_i \in F_p$ such that

\[
\overline{\alpha} = \sum_{i=1}^{f} b_i \overline{w}_i 
\]

This implies that

\[
\alpha = \sum_{i=1}^{f} b_i w_i + \pi
\]

We will finish this proof next class. \qed

3 Lecture 3 (Dillon Ethier)

In the following, $K$ is a finite extension of $Q_p$ of degree $n$. Denote by $A = \{x \in K : |x| \leq 1\}$ its ring of integers, and $M = \{x \in A : |x| < 1\} = (\pi)$ is the unique maximal ideal of $A$, where $\pi$ is a uniformizer. The ramification index of $K$ over $Q_p$ is $e$, and $A/M \cong F_p$.

Proposition 3.1. If $K$ is a finite extension of $Q_p$ of degree $n$, then $n = ef$. 

Proof. Since $A/M \cong \mathbb{F}_{p^f}$, we can choose a basis $\{w_i\}_{i=1}^f$ for $A/M$ over $\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p$, which we can lift to a set of coset representatives $\{w_i\}_{i=1}^f \subset A \setminus M$, i.e. $w_i \equiv \overline{w}_i \pmod{M}$. We claim that $B := \{w_i \pi^j : 1 \leq i \leq f, 0 \leq j \leq e - 1\}$ forms a basis for $K$ over $\mathbb{Q}_p$. The fact that $B$ is linearly independent over $\mathbb{Q}_p$ follows from the linear independence of $\{\overline{w}_i\}$ (exercise).

Now, to show that $B$ spans $K$ over $\mathbb{Q}_p$, it suffices to show that $B$ spans $A$ over $\mathbb{Z}_p$, so assume without loss of generality that $\alpha \in A$. Then $\overline{\alpha} := \alpha + M \subset A/M$ can be written as

$$\overline{\alpha} = \sum_{i=1}^f a_i \overline{w}_i,$$

where $\overline{w}_i \in \mathbb{F}_p$. We can lift each $\overline{w}_i$ to some $w_i \in \mathbb{Z}_p$. Lifting (1) back to $A$, this allows us to write $\alpha = \sum_{i=1}^f a_i w_i + \pi \alpha_1$, where $a_i \in \mathbb{Z}_p$ and $\alpha_1 \in A$. We can then repeat this process with $\alpha_1$ in place of $\alpha$, to obtain $\alpha_1 = \sum_{i=1}^f a_{i1} w_i + \pi \alpha_2$, where $a_{i1} \in \mathbb{Z}_p$ and $\alpha_2 \in A$. More generally, we have $\alpha_1 = \sum_{i=1}^f a_{i1} w_i + \pi \alpha_{t+1}$, where $a_{i1} \in \mathbb{Z}_p$, and $\alpha_{t} \in A$ for all $t \geq 1$. We can substitute back $l$ times in order to arrive at (for all $l \geq 1$)

$$\alpha = \sum_{i=1}^f w_i l^{t} a_{i} \pi^t + \pi^{l+1} \alpha_{l+1}.$$  

Now, since $\pi^e = p$, $\sum_{i=0}^t a_i \pi^t$ is a $\mathbb{Z}_p$-linear combination of $\{\pi^j\}_{j=0}^{e-1}$, and in turn $\beta_l := \sum_{i=1}^f w_i l^{t} a_{i} \pi^t$ is in the $\mathbb{Z}_p$-span of $B$. Thus, $|\alpha - \beta_l| = |\sum_{i=0}^t a_i \pi^i| = p^{-\frac{1}{e}} \to 0$ as $l \to \infty$, so it suffices to show that the span of $B$ is complete to show that it contains $\alpha$. This is an easy consequence of the fact that a finite dimensional normed vector space over a complete field is complete.

We have shown that $B$ is linearly independent and spans $K$ over $\mathbb{Q}_p$, hence it is a basis. Since $B$ has $ef$ elements, $n = ef$.

\begin{proposition}
Suppose $K/\mathbb{Q}_p$ is totally ramified, with $n = e$, and $\text{ord}_p(\pi) = 1/e$. Then $\pi$ satisfies an Eisenstein polynomial, i.e. a polynomial of the form

$$x^e + a_{e-1} x^{e-1} + \ldots + a_1 x + a_0,$$

where $a_i \in \mathbb{Z}_p, |a_i| < 1$, and $|a_0| = p^{-1}$.

**Proof.** First, note that $[\mathbb{Q}_p(\pi) : \mathbb{Q}_p] = e$, whence $1/e = \text{ord}_p(\pi) \in \frac{1}{[\mathbb{Q}_p(\pi) : \mathbb{Q}_p]} \mathbb{Z} \subseteq \frac{1}{[\mathbb{Q}_p(\pi) : \mathbb{Q}_p]} \mathbb{Z} \subseteq \frac{1}{e} \mathbb{Z}$.

Thus, $\pi$'s minimal polynomial over $\mathbb{Q}_p$ can be written in the form $g(x) = x^e + a_{e-1} x^{e-1} + \ldots + a_1 x + a_0$. If we denote by $\pi_1 := \pi, \pi_2, \ldots, \pi_e$ as the Galois conjugates of $\pi$ over $\mathbb{Q}_p$, then $g(x) = \prod_{i=1}^e (x - \pi_i)$, and

$$a_i = (-1)^{e-i} \sum_{1 \leq j_1 < \ldots < j_{e-i} \leq e} \pi_{j_1} \ldots \pi_{j_{e-i}}.$$  

In particular, since $|\pi| = p^{-1/e},$ we have $|a_i| \leq p^{-\frac{1}{e}} = p^{1} < 1$ whenever $i < e$. Since each $a_i \in M \cap \mathbb{Q}_p = p\mathbb{Z}_p,$ and $|a_0| = p^{-e/e} = p^{-1}$, the theorem is proved.  \hfill \Box

\begin{theorem}
1. Up to isomorphism, there is exactly one unramified extension of $\mathbb{Q}_p$ of degree $f$, which we will denote by $\mathbb{Q}_p^f$. It is equal to $\mathbb{Q}_p(\alpha)$, where $\alpha$ is a primitive root of $x^{p^f} - 1$.

2. Let $[K : \mathbb{Q}_p] = n = ef$, then $K = \mathbb{Q}_p^f(\pi)$, where $\pi$ satisfies an Eisenstein polynomial with $\mathbb{Q}_p^f$ coefficients.

**Proof.** 1. (existence) Let $\pi$ be a generator of $\mathbb{F}_p^*$, which is cyclic of order $p^f - 1$. Since $\mathbb{F}_p(\pi) = \mathbb{F}_{p^f}$, $\pi$ satisfies an irreducible polynomial of degree $f$ over $\mathbb{F}_p$, denote it $P(x) = x^f + \sum_{j=1}^{f-1} x^{f-j} + \ldots + \alpha x + \beta$, where $\alpha, \beta \in \mathbb{F}_p$. Now, lift $\overline{\pi}$ to any $a_i \in \mathbb{Z}_p$ with $a_i \equiv \overline{a}_i \pmod{p}$, to obtain $P(x) = x^f + a_{f-1} x^{f-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}_p[x]$. We know that $P(x)$ is irreducible over $\mathbb{Q}_p$ since $P(x)$ is irreducible over $\mathbb{F}_p$. Let $\alpha \in \overline{\mathbb{Q}_p}$ be a root of $P(x)$. We now make the definitions

$$\tilde{K} := \mathbb{Q}_p(\alpha), \quad \tilde{A} := \{a \in \tilde{K} : |a| \leq 1\} \quad \tilde{M} := \{a \in \tilde{A} : |a| < 1\}$$
Note that \( \alpha \in \bar{A} \) since \( \bar{A} \) is the integral closure of \( \mathbb{Z}_p \) in \( \bar{K} \).

By our construction, \( \alpha + \bar{M} \in \bar{A}/\bar{M} \) satisfies \( \mathcal{P}(x) \). Since \( \mathcal{P} \) is irreducible over \( \mathbb{F}_p \), we must have \( [\bar{A}/\bar{M} : \mathbb{F}_p] \geq f \).

However, from the previous lecture, we know that \( [\bar{A}/\bar{M} : \mathbb{F}_p] \leq [\bar{K} : \mathbb{Q}_p] = f \), and thus \( \bar{K} \) is unramified of degree \( f \).

We leave as an exercise the fact that \( \alpha \) is a primitive \( p^f - 1 \)th root of unity.

2. Let \( \pi \in K \) with \( \text{ord}_p(\pi) = 1/e \), and let \( E(x) \) be the monic minimal polynomial of \( \pi \) over \( \mathbb{Q}_{p'} \). Let \( \pi_1 := \pi, \pi_2, \ldots, \pi_r \) be conjugate roots of \( \pi \). Then \( E(x) = (x - \pi_1) \cdots (x - \pi_r) = x^r + a_{r-1}x^{r-1} + \ldots + a_1x + a_0 \). We have already established that \( \text{ord}_p(\pi_i) = 1/e \) independently of \( i \).

As we have done before, we note that \( |a_i| < 1 \) by the fact that each \( a_i \) can be written as a sum of products of the \( \pi_j \) and the strong triangle inequality.

Now, \( \text{ord}_p(a_0) = \text{ord}_p((-1)^r \pi_1 \cdots \pi_r) = \sum \text{ord}_p(\pi_i) = r/e \). But \( [K : \mathbb{Q}_{p'}] = e \), so \( r \leq e \), but also \( r > 0 \), so we must have \( \text{ord}_p(a_0) = 1 \). Thus \( E(x) \) is an Eisenstein polynomial over \( \mathbb{Q}_{p'} \), hence \( K \) is a totally ramified extension of \( \mathbb{Q}_{p'} \).

\[ \square \]

4 Lecture 4 - Brendan Murphy

5 Extensions of \( \mathbb{Q}_p \)

Last time, we proved that every extension \( K \) of \( \mathbb{Q}_p \) factors as a totally ramified extension of degree \( e \) over an unramified extension of degree \( f \), where \( e \) is the ramification index of \( K \) over \( \mathbb{Q}_p \) and \( f \) is the residue degree of \( K \) over \( \mathbb{Q}_p \). As a result, \( n = ef \). Further, we had that \( K = \mathbb{Q}_{p'}(\pi) \), where \( \pi \) is the uniformizer, and \( \mathbb{Q}_{p'} = \mathbb{Q}_p(\alpha) \), where \( \alpha \) is a lift of a generator of residue field of \( \mathbb{Q}_{p'} \) over \( \mathbb{Q}_p \).

5.1 Teichmüller Digits

The next corollary gives an explicit description of the elements of \( K \) as power series in \( \pi \) with digits in a set of roots of unity.

**Corollary 5.1.** Let \( K \) be a degree \( n \) extension of \( \mathbb{Q}_p \). Let \( A \subseteq K \) be the closed unit disk and let \( M \subseteq K \) be the open unit disk. Let \( e \) be the ramification index of the extension and let \( \pi \in A \) be the uniformizer, so that \( \text{ord}_p(\pi) = \frac{1}{e} \). Let \( f = [A/M : \mathbb{F}_p] \) be the residue degree of the extension.

Then

\[ K = \left\{ \sum_{i=0}^{\infty} a_i \pi^i : m \in \mathbb{Z}, a_i^{p^f} = a_i \right\} \quad \text{(3)} \]

\[ A = \left\{ \sum_{i=0}^{\infty} a_i \pi^i : a_i^{p^f} = a_i \right\} \quad \text{(4)} \]

\[ M = \left\{ \sum_{i=1}^{\infty} a_i \pi^i : a_i^{p^f} = a_i \right\} \quad \text{(5)} \]

The \( a_i \) are called **Teichmüller digits**. The proof of corollary 5.1 requires Hensel’s lemma, which we recall:

**Lemma 5.2 (Hensel’s Lemma).** Let \( f(x) = c_0x^n + \cdots + c_1x + c_0 \) be a polynomial with coefficients in \( \mathbb{Z}_p \). Suppose \( a_0 \) is a \( p \)-adic integer such that \( f(a_0) \equiv 0 \mod p \) and \( f'(a_0) \not\equiv 0 \mod p \). Then there exists a unique \( p \)-adic integer \( a \) such that \( f(a) = 0 \) and \( a \equiv a_0 \mod p \).

Note that we could replace \( \mathbb{Z}_p \) with any integral extension \( A \), and replace \( \equiv \mod p \) by \( \equiv \mod \pi \), where \( M = \langle \pi \rangle \) is the unique maximal ideal of \( A \). Now we proceed with the proof.

**Proof.** Note that if \( a^{p^f} = a \), then \( |a|_p = 1 \). Since \( |a_i \pi^i|_p = p^{-i/e} \), every power series of the form \( \sum_{i=m}^{\infty} a_i \pi^i \) converges to an element of \( K \). This shows that the set of power series on the right hand side of (3) is a subset of \( K \). To show the reverse inclusion, we must show that every element of \( K \) can be written as such a power series. Since every element of \( K \) can be written as \( \pi^m x \), where \( m \in \mathbb{Z} \) and \( x \in A \), it suffices to show that every element of \( A \) has the required form.

Fix a \( \beta \) in \( A \). We will expand \( \beta \) in powers of \( \pi \) using a process similar to finding the decimal expansion of a real number.

Let \( \beta \) the image of \( \beta \) in \( A/M \cong \mathbb{F}_{p^f} \). If \( \beta = 0 \), set \( a_0 = 0 \). Otherwise, \( \beta \) is a root of the polynomial \( f(x) = x^{p^f-1} - 1 \). By Hensel’s lemma, there exists a unique \( a_0 \) in \( A \) such that \( a_0 \equiv \beta \mod \pi \) and \( a_0^{p^f-1} = 1 \). Set \( a_1 = \beta - a_0 \pi \) so that \( \beta = a_0 + \pi a_1 \).
Since $\beta - a_0 \equiv 0 \mod \pi$, $\beta_1$ is an element of $A$, so we may apply the previous process to $\beta_1$. Let $\beta_1$ be the image of $\beta_1$ in $A/M$. If $\beta_1 = 0$, set $a_1 = 0$. Otherwise, by Hensel’s lemma there exists a unique $a_1$ in $A$ such that $a_1 \equiv \beta_1 \mod \pi$ and $a_1^{p^f-1} = 1$. Then

$$\beta = a_0 + a_1 \pi + \beta_2 \pi^2$$

where

$$\beta_2 := \frac{\beta_1 - a_1}{\pi}.$$  

Continuing in this way, we get a sequence of partial sums converging to $\beta$, since the remainder terms $\beta_k \pi^k$ tend to zero. 

Remark. This description shows us that the elements of $K$ are just like the elements of $\mathbb{Q}_p$: the elements of $K$ are power series in the uniformizer $\pi$ with a set of digits.

Recall that $\mathbb{Q}_{p^f} = \mathbb{Q}_p(\alpha)$, where $\alpha$ is a primitive $(p^f - 1)^{th}$ root of unity. We found $\alpha$ by lifting a generator $\bar{\alpha}$ from the multiplicative group $\mathbb{F}_{p^f}^\times$ of the residue field $A/M$. Since $\{\bar{\alpha}, \bar{\alpha}^2, \ldots, \bar{\alpha}^{p^f-1}\}$ are distinct elements of $\mathbb{F}_{p^f}$, the lifts $\{\alpha, \alpha^2, \ldots, \alpha^{p^f-1}\}$ are distinct elements of $\mathbb{Q}_{p^f}$.

Also, note that each $\alpha^k$ is a $(p^f - 1)^{th}$ root of unity, and that $\alpha^k$ is a primitive root if $k$ is relatively prime to $p^f - 1$. Since $\mathbb{Q}_{p^f}$ is the unique unramified degree $f$ extension of $\mathbb{Q}_p$, the $\alpha^k$ are the only $p^f$ roots of unity in $\mathbb{Q}_{p^f}$, which means that the Teichmüller digits $a_i$ from corollary 5.1 are actually powers of $\alpha$. (We could also see this from Hensel’s lemma.) It’s useful to define a function giving us $\alpha$ from $\mathbb{F}_{p^f}$.

Definition 5.3 (Teichmüller lift). We define a map Teich from $\mathbb{F}_{p^f}$ into $\mathbb{Q}_{p^f}$ by $\text{Teich}(0) = 0$ and $\text{Teich}(\bar{\alpha}^i) = \alpha^i$ for $i = 0, \ldots, p^f - 1$.

Note that the image of Teich is actually in $\mathbb{Z}_{p^f}$.

It’s easy to see that Teich is a group homomorphism from $\mathbb{F}_{p^f}^\times$ into $\mathbb{Q}_{p^f}^\times$. In fact, since $\bar{\alpha}$ is a primitive $(p^f - 1)^{th}$ root in $\mathbb{F}_{p^f}$ and $\alpha$ is a primitive $(p^f - 1)^{th}$ root in $\mathbb{Q}_{p^f}^\times$, Teich is an isomorphism onto its image.

Just like the conjugates of $\bar{\alpha}$ in $\mathbb{F}_{p^f}$ are $\bar{\alpha}, \bar{\alpha}^p, \bar{\alpha}^{p^2}, \ldots, \bar{\alpha}^{p^f-1}$, the conjugates of $\alpha = \text{Teich}(\bar{\alpha})$ are $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^f-1}$.

5.2 The completion of $\overline{\mathbb{Q}}_p$

Unlike the real numbers, the algebraic closure of $\mathbb{Q}_p$ is not complete. Here we give a summary of the completion of $\mathbb{Q}_p$.

The completion is created in the usual by isometrically embedding $\overline{\mathbb{Q}}_p$ into the space of (equivalence classes) of Cauchy sequences in $\overline{\mathbb{Q}}_p$. We call the completion $\mathbb{C}_p$. Fortunately, $\mathbb{C}_p$ is algebraically closed so the madness ends\(^1\).

6 $p$-adic Power Series

Consider

$$f(x) = \sum_{k=0}^{\infty} a_k x^k,$$

where the $a_k$ are elements of $\mathbb{C}_p$. We define the radius of convergence of $f$ by

$$r := \frac{1}{\limsup_{k \to \infty} |a_k|^{1/k}}$$

or

$$\text{ord}_p(r) = \liminf_{k \to \infty} \left( \frac{1}{k} \text{ord}_p(a_k) \right).$$

These definitions are equivalent, since $\limsup_{n} a_n - a_n = \liminf_{n} a_n$:

$$\frac{1}{r} = \limsup_{k} |a_k|^{1/k} = \limsup_{k} p^{-\frac{1}{k} \text{ord}_p(a_k)} = \limsup_{k} (-\frac{1}{k} \text{ord}_p(a_k)) = \liminf_{k} (\frac{1}{k} \text{ord}_p(a_k)),$$

hence

$$\text{ord}_p(r) = -\text{ord}_p\left(\frac{1}{r}\right) = -\text{ord}_p\left(p^{-\liminf_{k} (\frac{1}{k} \text{ord}_p(a_k))}\right) = \liminf_{k} \left(\frac{1}{k} \text{ord}_p(a_k)\right).$$

The following proposition justifies the term “radius of convergence:

\(^1\)... or nearly ends: some people worry about the spherical completion of $\overline{\mathbb{Q}}_p$, which is sometimes denoted $\Omega_p$. A spherically complete metric space has the property that every nested sequence of closed balls with finite radius has a non-empty intersection. This property is needed to prove the Hahn-Banach theorem, and the topological completion $\mathbb{C}_p$ does not possess it.
Lemma 6.2. Let \( p \) be a prime number. Since \( \text{ord}_p(n) \) is the \( p \)-adic order of \( n \) in \( \mathbb{Z} \), we have \( \text{ord}_p(n) = \frac{n - \sigma(n)}{p - 1} \).

Proposition 6.1. Let \( A \) be an integral domain. Then \( A \) is a field if and only if \( A \) is an integral domain and every non-zero element has a multiplicative inverse.

Proof. Use the root test, or see Koblitz p.76.

Power series with "integral" coefficients always have a radius of convergence of at least 1:

Proposition. Let \( K \) be a finite extension of \( \mathbb{Q}_p \) and let \( f \) be a power series in \( A[[x]] \), then \( f \) converges for all \( x \) in \( M \).

Proof. Let \( f = \sum_{k=0}^\infty a_k x^k \). Since \( a_k \in A \), \( |a_k| \leq 1 \). Hence \( \limsup_k |a_k|^{1/k} \leq 1 \), which implies that the radius of convergence of \( f \) is at least 1.

In particular, if \( f \in \mathbb{Z}[[x]] \) then \( f \) converges for all \( x \) in \( \mathbb{C}_p \) with \( |x| < 1 \).

6.1 The \( p \)-adic Exponential and Logarithm

We define the exponential function by its usual series:

\[
\exp(x) := \sum_{n=0}^\infty \frac{x^n}{n!}.
\]

Over \( \mathbb{R} \) or \( \mathbb{C} \) the exponential has an infinite radius of convergence, because the factorials in the denominator grow very quickly. However, over \( p \)-adic fields \( \mathbb{N} \) is very small because it has many factors of \( p \), so \( \frac{1}{n!} \) is very large.

Proposition. \( \exp(x) \) converges for \( |x| < p^{-\sigma(n)} \).

Note that \( \exp \) only converges on a disk much smaller than the unit disk. To determine the radius of convergence, we first need to know the \( p \)-adic order of \( n! \). Let \( n \) be a positive integer with \( p \)-adic expansion \( n = b_0 + b_1 p + \cdots + b_\ell p^\ell \), where \( b_i \in \{0, 1, \ldots, p-1\} \). Define \( \sigma(n) = b_0 + b_1 + \cdots + b_\ell \).

Lemma 6.2. Let \( n \) be a positive integer and let \( \sigma(n) \) be defined as above. Then

\[
\text{ord}_p(n!) = \frac{n - \sigma(n)}{p - 1}.
\]

Proof. The claim is true for \( n = 1 \). Let \( n > 1 \) be an integer and assume that

\[
\text{ord}_p((n-1)!) = \frac{n - 1 - \sigma(n-1)}{p - 1}.
\]

Write \( n \) as \( n = b_0 + b_1 p + \cdots + b_\ell p^\ell \). If \( p \nmid n \), then \( b_0 > 0 \), hence \( n - 1 = (b_0 - 1) + b_1 p + \cdots + b_\ell p^\ell \). Then \( \text{ord}_p(n!) = \text{ord}_p(n) + \text{ord}_p((n-1)! = \text{ord}_p((n-1)! \). Hence

\[
\text{ord}_p(n!) = \frac{n - 1 - \sigma(n-1)}{p - 1} = \frac{n - 1 - (b_0 - 1 + b_1 + \cdots + b_\ell)}{p - 1} = \frac{n - (b_0 + b_1 + \cdots + b_\ell)}{p - 1} = \frac{n - \sigma(n)}{p - 1}.
\]

If \( p^k \mid n \) for some \( k \geq 1 \), then \( n = b_k p^k + \cdots + b_\ell p^\ell \), where \( b_k \geq 1 \). It follows that \( n - 1 = (b_k p^k + \cdots + b_\ell p^\ell) - 1 = p^k - 1 + (b_k - 1)p^k + \cdots + b_\ell p^\ell = (p - 1)(1 + p + \cdots + p^{k-1}) + (b_k - 1)p^k + \cdots + b_\ell p^\ell \). Hence

\[
\text{ord}_p(n!) = \frac{n - 1 - \sigma(n-1)}{p - 1} = \frac{n - 1 - (k(p-1) + b_k - 1 + b_{k+1} + \cdots + b_\ell)}{p - 1}.
\]

Since \( \text{ord}_p(n!) = \text{ord}_p(n) + \text{ord}_p(n-1) = k + \text{ord}_p(n-1) \), we have

\[
\text{ord}_p(n!) = k + \frac{n - 1 - (k(p-1) + b_k - 1 + b_{k+1} + \cdots + b_\ell)}{p - 1} = \frac{n - 1 - (b_k - 1 + b_{k+1} + \cdots + b_\ell)}{p - 1} = \frac{n - \sigma(n)}{p - 1}.
\]

\[\square\]
Now we can compute the radius of convergence of the $p$-adic exponential series.

**Proof of proposition 6.1.** Let $r$ denote the radius of convergence. Then

$$\text{ord}_p(r) = \liminf_{k \to \infty} \left( \frac{1}{k} \text{ord}_p \left( \frac{1}{k!} \right) \right)$$

$$= \liminf_{k \to \infty} \left( \frac{1}{k} \left( \frac{1}{p-1} - \sigma(k) \right) \right)$$

$$= \liminf_{k \to \infty} \left( \frac{-1}{p-1} + \frac{\sigma(k)}{k(p-1)} \right).$$

If $k = b_0 + b_1 p + \cdots + b_\ell p^\ell$, then $b_i \leq p - 1$ for $i = 0, \ldots, \ell$ and $\ell \leq \log_p(k)$, so $\sigma(k) \leq (p-1) \log_p(k)$. Hence $\sigma(k)/k \to 0$ as $k \to \infty$, and we have $\text{ord}_p(k) = -1/(p-1)$. Thus $\exp(x)$ converges for $|x| < p^{-\frac{1}{p-1}}$, as desired.

**Remark.** We can’t analytically continue power series over $\mathbb{C}_p$ like we can over $\mathbb{C}$, because in $\mathbb{C}_p$ neighborhoods do not overlap—they are either concentric or disjoint.

We also define the logarithm in terms of its power series:

**Definition 6.3.** $\log(1 - x) := -\sum_{n=1}^{\infty} \frac{x^n}{n}.$

Later we will show that $\log(1 - x)$ converges for $|x| < 1$ and diverges otherwise.

**Proposition.** $\exp$ and $\log$ are inverses on $|x| < p^{-\frac{1}{p-1}}$.

**Proof.** Koblitz p. 81

To be precise, for $|x| < 1$ we have $\log(1 - (\exp(x) + 1)) = x$ and $\exp(\log(1 - x)) = 1 - x$. 

### 6.2 Newton Polygons

Newton polygons are a geometric way of immediately seeing the radius of convergence, and more.

Let $f(x) = 1 + \sum_{k=1}^{\infty} a_k x^k \in 1 + x \mathbb{C}_p[[x]]$. Define the Newton polygon of $f$ as the lower convex hull of the points $(k, \text{ord}_p(a_k))$ and $(0, 0)$ in $\mathbb{R}^2$. We can think of the lower convex hull as what we get by shrink wrapping the points from below.

**Example 6.1.** Let $f(x) = 1 + p^{-1} x + p^2 x^3 + p^2 x^4$. The Newton polygon of $f$ is the lower convex hull of the points $(0, 0), (1, -1), (2, \infty), (3, 2), (4, 2)$.
The roots of a polynomial are determined up to units by its Newton polygon:

**Proposition.** Let \( f(x) = (1 - \alpha_1 x) \cdots (1 - \alpha_n x) \in \mathbb{C}_p[x] \). Set \( \lambda_k = \text{ord}_p(\alpha_k) \). If \( \lambda \) is a slope of the Newton polygon of \( f \) of length \( \ell \), then there are exactly \( \ell \) reciprocal roots \( \alpha_k \) with \( \lambda_k = \lambda \).

**Proof.** Deferred. \( \square \)

Thus the polynomial \( f \) from the previous example has three roots of \( p \)-adic order 1, and one root of \( p \)-adic order \( -1 \).

**Term.** We call \( \text{ord}_p(\alpha) \) the *slope* of \( \alpha \).

The Newton polygon of a polynomial is always bounded by a finite number of finite segments. If we consider the Newton polygon of a power series \( f(x) \in 1 + x\mathbb{C}_p[[x]] \) with infinitely many non-zero coefficients, then there are two options:

1. the Newton polygon of \( f \) consists of infinitely many lines segments, or
2. the Newton polygon of \( f \) contains an infinitely long segments.

**Example 6.2.** The Newton polygon of the power series \( 1 + \sum_{k=1}^{\infty} p x^k \) consists of two segments:
7 Lecture 5 - Siegfred

Binomial Series

Definition: If \( x, \alpha \in \mathbb{C}_p \), define

\[
(1 + x)^\alpha := \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n,
\]

where \( \binom{\alpha}{0} := 1 \) and \( \binom{\alpha}{n} := \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!} \).

Proposition. If \( \alpha \in \mathbb{Z}_p \) then \( \binom{\alpha}{n} \in \mathbb{Z}_p \). Consequently, \( (1 + x)^\alpha \) converges for \( |x| < 1 \).

Proof. The key here is to use continuity of the norm together with the fact that \( \mathbb{Z} \) is dense in \( \mathbb{Z}_p \) (by Theorem 2 in §I.4 of Koblitz). The addition and multiplication operations are continuous functions from \( \mathbb{C}_p \times \mathbb{C}_p \to \mathbb{C}_p \) with the \( p \)-adic norm \(| \cdot |_p\) (the proof of this is the same as the proof that the same operations are continuous on \( \mathbb{R} \) or \( \mathbb{C} \)). Thus the function \( g : x \mapsto \binom{\alpha}{n} \) is continuous since it is a topology. Let \( \{a_i\} \) now be a sequence of integers that tend to \( \alpha \) in \( \mathbb{Q}_p \). By continuity,

\[
|g(\alpha)|_p = \lim_{i \to \infty} |g(a_i)|_p.
\]

Since \( a_i \), and thus \( g(a_i) \), is an integer for each \( i \), it follows that the expression on the right has value at most 1. Thus \( |g(\alpha)|_p \) is at most 1 and so \( g(\alpha) \in \mathbb{Z}_p \) by definition of \( \mathbb{Z}_p \). This proves the first statement. The second statement follows immediately since each term of the series has norm at most \( |x|^n \), which tends to 0 for \( |x| < 1 \) (recall that a series converges in \( \mathbb{C}_p \) if and only if the norms of the terms tend to 0).

Let us now apply the above proposition to get

Proposition. If \( \zeta \) is a primitive \( p \)-th root of unity and \( \alpha \in \mathbb{Z}_p \), then \( \zeta^\alpha \in \mathbb{Z}_p \).

Proof. By the above proposition, it suffices to show that \( \zeta = 1 + \pi \) with \( |\pi| < 1 \). To this end, set \( K = \mathbb{Q}_p(\zeta) \) and let \( A := \{x \in K : |x| \leq 1\} \) and \( M := \{x \in K : |x| < 1\} \) so that \( A/M \) is the residue field of \( K \), isomorphic to \( \mathbb{F}_{p^f} \) for some \( f \leq p \) (this appeals to a previously proved proposition on the structure of \( p \)-adic fields). Since \( \zeta^p = 1 \), it follows that \( (\zeta + M)^p = (1 + M)^p \) in the residue field. Now the map \( x \mapsto x^p \) is a group automorphism of the cyclic group \( \mathbb{F}_{p^f}^\times \) because \( p^f - 1 \) and \( p \) are relatively prime (in fact it is a field automorphism of \( \mathbb{F}_{p^f} \) by the binomial theorem because \( \mathbb{F}_{p^f} \) has characteristic \( p \) and since nonzero field homomorphisms are injective and injective maps of finite sets are surjective). Hence \( \zeta + M = 1 + M \), i.e. \( \zeta - 1 \in M \), but this means \( |\zeta - 1| < 1 \) by definition of \( M \).

Theorem. Let \( f(x) = (1 - \alpha_1 x) \cdots (1 - \alpha_n x) \) be a polynomial in \( \mathbb{C}_p[x] \). Set \( \lambda_i = \text{ord}_p(\alpha_i) \) for each \( i \). If \( \lambda \) is a slope of the Newton polygon of \( f \) of horizontal length \( \ell \), then there are exactly \( \ell \) reciprocal roots \( \alpha_i \) with \( \lambda_i = \lambda \).

Proof. Relabel so that \( \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n \). The idea is to use the ultrametric inequality on the expression of the coefficients of \( f \) in terms of the reciprocal roots to get bounds on the \( y \)-coordinates of the points of the Newton polygon. First we show that if \( \lambda_1 = \cdots = \lambda_r < \lambda_{r+1} \) then the first segment of the Newton polygon has is the line segment from \((0,0)\) to \((r, r\lambda_1)\) (and thus has slope \( \lambda_1 \)). Write

\[
f(x) = 1 + a_1 x + \cdots + a_n x^n,
\]
so that, for $i = 1, \ldots, n$,
\[ a_i = (-1)^i \sum \alpha_{j_1} \cdots \alpha_{j_i}, \]
with the sum over all $i$-tuples $(j_1, \ldots, j_i)$ with $0 \leq j_1 < \cdots < j_i \leq n$. The ultrametric inequality thus gives, for $i = 1, \ldots, n$,
\[
\text{ord}_p(a_i) \geq \min_{(j_1, \ldots, j_i)} \text{ord}_p(\alpha_{j_1} \cdots \alpha_{j_i}) \\
= \min_{(j_1, \ldots, j_i)} (\lambda_{j_1} + \cdots + \lambda_{j_i}) \\
\geq i \lambda_1.
\]
This implies that the point $(i, \text{ord}_p(a_i))$ in the Newton polygon is above (or the same as) the point $(i, i \lambda_1)$ for all $i = 1, \ldots, n$. Now we set $i = r$ in the above computation and use

**Lemma.** If $\text{ord}_p(a) < \text{ord}_p(b)$ then $\text{ord}_p(a + b) = \text{ord}_p(a)$.

**Proof.** (Supplied by typist): The ultrametric inequality gives, since $a = a + b - b$, $\text{ord}_p(a) \geq \text{ord}_p(a + b)$ or $\text{ord}_p(a) \geq \text{ord}_p(b)$; since the latter is false, the former is true. Also, the ultrametric inequality again gives $\text{ord}_p(a + b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\} = \text{ord}_p(a)$. Thus $\text{ord}_p(a + b) = \text{ord}_p(a)$.

If the $r$-tuple $(j_1, \ldots, j_r)$ has a coordinate greater than $r$ then $\lambda_{j_1} + \cdots + \lambda_{j_r} > r \lambda_1$ by definition of $r$. Hence, in the sum expression
\[ a_r = (-1)^r \sum \alpha_{j_1} \cdots \alpha_{j_r}, \]
the term with the least order $r \lambda_1$ is the term with $(j_1, \ldots, j_r) = (1, \ldots, r)$; all other terms have order strictly greater than $r \lambda_1$. Hence the lemma gives $\text{ord}_p(a_r) = r \lambda_1$, and so the point $(i, \text{ord}_p(a_r))$ is precisely the point $(r, r \lambda_1)$. On the other hand, if $i > r$, then applying again the ultrametric inequality,
\[
\text{ord}_p(a_i) \geq \min_{(j_1, \ldots, j_i)} \text{ord}_p(\alpha_{j_1} \cdots \alpha_{j_i}) \\
= \min_{(j_1, \ldots, j_i)} (\lambda_{j_1} + \cdots + \lambda_{j_i}) \\
\geq i \lambda_1
\]
because each $i$-tuple $(j_1, \ldots, j_i)$ necessarily has a coordinate $j_k$ greater than $r$ and so has the corresponding $\lambda_{j_k}$ strictly greater than $\lambda_1$. In particular, the point $(r + 1, \text{ord}_p(a_{r+1}))$ is strictly above $(r + 1, (r + 1) \lambda_1)$. This shows that the first segment of the Newton polygon of $f$ is the line segment from $(0,0)$ to $(r,r \lambda_1)$.

Next, to get the second segment, suppose that $\lambda_{r+1} = \cdots = \lambda_s < \lambda_{s+1}$. If $i \geq r + 1$ then the least possible value of $\text{ord}_p(\alpha_{j_1} \cdots \alpha_{j_i})$ in the sum expression for $a_i$ is attained when $(j_1, \ldots, j_i) = (1, \ldots, i)$, and so this value is at least $r \lambda_1 + (i - r) \lambda_{r+1}$; thus the point $(i, \text{ord}_p(a_i))$ is above $(i, r \lambda_1 + (i - r) \lambda_{r+1})$. When $i = s$ then all $(j_1, \ldots, j_s) \neq (1, \ldots, s)$ in the sum expression for $a_s$ will have $\text{ord}_p(\alpha_{j_1} \cdots \alpha_{j_s}) > r \lambda_1 + (s - r) \lambda_{r+1}$ since at least one $j$ will be larger than $s$, so by the above lemma, $\text{ord}_p(a_s) = r \lambda_1 + (s - r) \lambda_{r+1}$; thus the point $(s, \text{ord}_p(a_s))$ is precisely $(s, r \lambda_1 + (s - r) \lambda_{r+1})$. When $i > s$ then all $(j_1, \ldots, j_i)$ in the sum expression for $a_i$ will have at least one $j$ larger than $s$, so in this case $\text{ord}_p(a_i) > r \lambda_1 + (i - r) \lambda_{r+1}$. Hence the second segment of the Newton polygon of $f$ is the line segment from $(r, r \lambda_1)$ to $(s, r \lambda_1 + (s - r) \lambda_{r+1})$, with slope $\lambda_{r+1}$. To get the third segment, suppose that $\lambda_{s+1} = \cdots = \lambda_t < \lambda_{t+1}$, and we use the ultrametric inequality similarly to get
\[
\text{ord}_p(a_i) \geq r \lambda_1 + (s - r) \lambda_{r+1} + (i - s) \lambda_{s+1} \quad \text{for } i \geq s + 1 \\
\text{ord}_p(a_i) = r \lambda_1 + (s - r) \lambda_{r+1} + (i - s) \lambda_{s+1} \quad \text{for } i = t \\
\text{ord}_p(a_i) > r \lambda_1 + (s - r) \lambda_{r+1} + (i - s) \lambda_{s+1} \quad \text{for } i \geq t + 1
\]
and conclude that the third segment of the Newton polygon of $f$ is the line segment from $(s, r \lambda_1 + (s - r) \lambda_{r+1})$ to $(t, r \lambda_1 + (s - r) \lambda_{r+1} + (t - s) \lambda_{s+1})$, with slope $\lambda_{s+1}$. We proceed in this way until we exhaust all the $\lambda_i$'s.

Newton polygons of power series

There are two things that can happen for a Newton polygon of a $p$-adic power series. One possibility is for it to have only finitely long line segments. This happens if the power series has only finitely many terms, i.e. is a polynomial. An example of a power series with infinitely many terms for which this happens is $\sum p^i x^i$, since for this case $\text{ord}_p(a_i) = \text{ord}_p(p^i) = i^2$ and so the slopes of the Newton polygon from $i$ to $i + 1$ increase to $\infty$ with $i$. The other possibility is for the Newton polygon to have an infinitely long line. The connection between the slopes of the Newton polygon and the radius of convergence of the power series is given in the following.
Proposition. Let \( f = \sum a_i x^i \) be a \( p \)-adic power series. If \( \varepsilon \) is the supremum of the slopes of the line segments and line (if there is one) of the Newton polygon of \( f \), then the radius of convergence of \( f \) is \( p^{-\varepsilon} \).

Proof. (It was only shown in class that the radius of convergence is at least \( p^\varepsilon \); the reader is referred to Koblitz for the proof that it is at most \( p^\varepsilon \).) To show that the power series converges for \( |x| < p^\varepsilon \), the idea is that if \( \varepsilon > 0 \) and \( i \) is large enough then the Newton polygon of \( f \) from \( i \) to \( i + 1 \) will have slope larger than \( b - \varepsilon \) and so will be above some line with slope \( b - \varepsilon \). Note \( |x| < p^\varepsilon \) if and only if \( \text{ord}_p(x) > -b \). Write \( \lambda = \text{ord}_p(x) \) and suppose \( |x| < p^\varepsilon \), so that \( b > \lambda \). Let \( b > \lambda_1 > -\lambda \), and let \( j \geq 1 \) such that the slope of the Newton polygon from \( j \) to \( j + 1 \) is larger than \( \lambda_1 \). Then all points of the Newton polygon \( P \) of \( f \) with \( x \)-coordinate larger than \( j \) will be above or at the line with slope \( \lambda_1 \) passing through \( (i, P(i)) \). Thus, for some real number \( c \), if \( i \geq j \) then

\[
\text{ord}_p(a_i x^i) = \text{ord}_p(a_i) + i \lambda \geq \lambda_1 i + c + i \lambda.
\]

The expression at the right goes to \( \infty \) with \( i \) since \( \lambda_1 + \lambda > 0 \). Hence \( \text{ord}_p(a_i x^i) \to \infty \), i.e. \( |a_i x^i|_p \to 0 \). Thus \( \sum a_i x^i \) converges (recall that a \( p \)-adic series converges if and only if its terms go to \( 0 \)).

\[ \square \]

Theorem (\( p \)-adic Weierstrass preparation theorem). Let \( f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i \) be in \( \mathbb{C}_p[[x]] \). Suppose that the Newton polygon of \( f \) changes slope at \( i = N \) and the slope of the line segment of the Newton polygon of \( f \) from \( N \) to \( N + 1 \) is \( \lambda \). Then there is a polynomial \( h \in 1 + x \mathbb{C}_p[x] \) of degree \( N \) and a \( g \in 1 + x \mathbb{C}_p[[x]] \) such that \( f(x) = h(x)g(x) \) and \( g(x) \) is nonzero for \( |x| < p^\lambda \). Furthermore, the Newton polygon of \( h \) is the same as the Newton polygon of \( f \) from \( 0 \) to \( N \) (which is the part of the Newton polygon of \( f \) with slopes less than \( \lambda \)).

(The proof was not discussed in class).

One way to visualize the above theorem is that to each line segment of the Newton polygon of \( f \) there is a polynomial \( h \) with degree equal to the horizontal length of the line segment and such that \( h \) is a factor of \( f \). For example, if the Newton polygon of \( f \) has three line segments with increasing slopes \( d_1, d_2, d_3 \) and an infinite line with slope \( \lambda \), then there are polynomials \( h_1, h_2, h_3 \) with degrees \( d_1, d_2, d_3 \) respectively, such that we can factor \( f \) as

\[ f = h_1 h_2 h_3 g \]

with \( g(x) \) nonzero for \( |x| < p^\lambda \). Thus, all \( p \)-adic entire functions are precisely

\[ \prod_{i=1}^{\infty} (1 - \alpha_i x), \quad \text{with} \quad \alpha_i \to 0 \]

(the details are in Koblitz).

\( p \)-adic analytic representation of an additive character on \( \mathbb{F}_q \)

We first recall the definition of the trace of an element of a field extension \( E/F \). Let \( E \) be a finite separable extension of the field \( F \). For \( \alpha \in E \), define the linear map \( T_\alpha : E \to E \) by multiplication by \( \alpha \), i.e.

\[ T_\alpha : x \mapsto \alpha x. \]

Define the trace of \( \alpha \) over \( F \) by

\[ \text{Tr}_{E/F}(\alpha) := \text{Trace}[T_\alpha], \]

where \([T_\alpha]\) is the matrix representation of \( T_\alpha \) as a linear map \( E \to E \), with respect to any basis of \( E \) as a vector space over \( F \) (recall that Trace:AB = Trace:BA by direct computation, so the trace of similar matrices are equal, so this definition does not depend on the choice of basis of \( E/F \)). Two other definitions, equivalent to the above definition, of the trace are (as in chapter 7 of Ash):

\[ \text{Tr}_{E/F}(\alpha) = [E : F(\alpha)] \sum_{i=1}^{[F(\alpha):F]} \alpha_i, \]

where the \( \alpha_i \) are the Galois conjugates of \( \alpha \), counting multiplicity, over any splitting field of its minimal polynomial over \( F \), and

\[ \text{Tr}_{E/F}(\alpha) = \sum_{i=1}^{[E:F]} \sigma_i(\alpha), \]
where the $\sigma_i$ are the distinct $F$-embeddings of $E$ into a normal extension of $E$.

**Example 1:** Let $E = \mathbb{F}_q$ where $q = p^a$ for some prime $p$ and integer $a \geq 1$. Recall that $E/F$ is a splitting field of a separable polynomial and thus a Galois extension. The generator of the Galois group of $E/F$ is the Frobenius map $\sigma : x \mapsto x^p$ (because the Galois group has order $a$ and $x \mapsto x^{p^j}$ cannot be the identity for $j < a$ since the polynomial $x^{p^j} - x$ has at most $p^j$ roots). Thus, for $\alpha \in E$,

$$\text{Tr}_{E/F}(\alpha) = \sum_{j=0}^{a-1} \sigma^j(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{a-1}}.$$ 

**Example 2:** Let $E = \mathbb{Q}_p(\alpha)$, where $\alpha$ is a Teichmüller representative of $\alpha \in \mathbb{F}_q$, $q = p^a$, so that $\alpha^{p^a-1} = 1$. Then

$$\text{Tr}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{a-1}}.$$ 

Note: The trace of $\alpha \in \mathbb{Q}_p$ that is integral over $\mathbb{Z}$ is in $\mathbb{Z}_p$, which is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ (because the trace of an integral element is integral).

## 8 Lecture 6 - Jamie

Recall:

- $\alpha = \text{Teich}(\bar{\alpha})$ means $\alpha \equiv \bar{\alpha} \mod p$ and $\alpha^{p^a-1} = 1$.

- If $\bar{\alpha} \in \mathbb{F}_q$, where $q = p^a$, then $\text{Tr}_{E/F}(\bar{\alpha}) = \bar{\alpha} + \bar{\alpha}^p + \cdots + \bar{\alpha}^{p^{a-1}}$. Also, if $\bar{\alpha} \in \mathbb{Q}_p$ and $\alpha = \text{Teich}(\bar{\alpha})$ then $\text{Tr}_{\mathbb{Q}_p/\mathbb{Q}_p}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{a-1}} \in \mathbb{Z}_p$ and $\text{Tr}(\bar{\alpha}) \equiv \text{Tr}(\alpha) \mod p$.

Let $\zeta_p$ be a primitive $p$-th root of unity. Define an additive character $\psi : \mathbb{F}_q \to \mathbb{C}_p$ by $\psi(x) = \zeta^\text{Tr}_{E/F}(x)$. From above, if $\bar{\alpha} \in \mathbb{F}_q$ and $\alpha = \text{Teich}(\bar{\alpha})$, then 

$$\zeta^\text{Tr}_{E/F}(\bar{\alpha}) = \zeta^\text{Tr}_{\mathbb{Q}_p/\mathbb{Q}_p}(\alpha)$$

We saw last time, using binomial series, that $\zeta^\text{Tr}_{\mathbb{Q}_p/\mathbb{Q}_p}(\alpha)$ makes sense. So we have $\psi : \mathbb{F}_q \to \mathbb{C}_p$ by $\psi(x) = \zeta^\text{Tr}_{\mathbb{Q}_p/\mathbb{Q}_p}(\text{Teich}(x))$. We will come back to this later.

**Definition 8.1.** Define the Artin-Hasse exponential:

$$E(t) := \exp(\sum_{n=0}^{\infty} \frac{\alpha^n}{p^n}) \in \mathbb{Q}[t]$$

**Proposition 8.2.** $E(t) \in 1 + t + t^2(\mathbb{Z}_p \cap \mathbb{Q})[[t]]$ (hence $E(t)$ converges on $|x| < 1$)

**Proof.** Fact: (Dierdonne-Dwork Lemma) Let $f \in 1 + t\mathbb{Q}_p[[t]]$, then the coefficients of $f$ are in $\mathbb{Z}_p$ iff $\frac{f(t)^p}{f(t)} \in 1 + pt\mathbb{Z}_p[[t]]$ (cf in Koblitz p. 93). Consider

$$\frac{E(t)^p}{E(t)} = \frac{\exp(p \sum_{n=0}^{\infty} \frac{\alpha^n}{p^n})}{\exp(p \sum_{n=0}^{\infty} \frac{\alpha^n}{p^n})} = e^{pt} = \sum_{n=0}^{\infty} \frac{p^n t^n}{n!}.$$ 

Since $\text{ord}_p\left(\frac{p^n}{n!}\right) = n - \text{ord}_p(n!) = n - \frac{n - \sigma(n)}{p-1} = n \frac{p-2}{p-1} + \frac{\sigma(n)}{p-1} \geq 1$ for $n \geq 1$ we have $e^{pt} \in 1 + pt\mathbb{Z}_p[[t]]$.

**Definition 8.3.** Define for $b > 0$ and $c \in \mathbb{R}$

$$L(b; c) = \{\sum_{i=0}^{\infty} a_i t^i | a_i \in \mathbb{C}_p, \text{ord}_p(a_i) \geq bi + c\}$$

Then for any element of $L(b;c)$, the Newton polygon lies above the line $y = bx + c$ and it converges for $|x| < p^b$ (which includes the unit disc since $b > 0$).

**Definition 8.4.** A function is called **overconvergent** if it belongs to $L(b; c)$ for some $b > 0$, $c \in \mathbb{R}$.

Note: $L(b_1; c_1) \cdot L(b_2; c_2) \subseteq L(\min(b_1, b_2); c_1 + c_2)$, in particular, $L(b; 0)$ is a ring.

**Definition 8.5.** Define a **splitting function** $\theta(t)$ as any function such that

1. $\theta(t) \in L(b; c)$ some $b > 0$, $c \in \mathbb{R}$
2. \( \theta(1) \) is a primitive \( p \)-th root of unity.

3. if \( \hat{t} = \text{Teich}(\tilde{t}) \) (meaning \( \hat{t}^p = 1 \), then \( \theta(1)^{\text{Tr}_{K_{p/\hat{t}}}^K(\tilde{t})} = \theta(\hat{t})\theta(\tilde{t})\ldots\theta(\hat{t}^{p^{-1}}) \))

In other words, \( \psi : \mathbb{F}_q \to \mathbb{C}_p \) by \( \psi(x) = \theta(\hat{x})\theta(\tilde{x})\ldots\theta(\hat{x}^{p^{-1}}) \) is an additive character.

**Construction of Dwork’s splitting functions**

Let \( s \in \mathbb{Z}_{\geq 1} \cup \{+\infty\} \). Define

\[
E_s(t) := \exp(\sum_{n=0}^{\infty} \frac{t^n}{p^n})
\]

Consider

\[
t(1 + \frac{t^{p-1}}{p^1} + \frac{t^{p^2-1}}{p^2} + \cdots + \frac{t^{p^{s-1}-1}}{p^{s-1}})
\]

the Newton polygon of

\[
(1 + \frac{t^{p-1}}{p^1} + \frac{t^{p^2-1}}{p^2} + \cdots + \frac{t^{p^{s-1}-1}}{p^{s-1}})
\]

has first segment joining the points \((0, 0)\) and \((p-1, -1)\), so it has slope \(-\frac{1}{p-1}\). By Newton polygon theory there exists \((p-1)\) reciprocal roots with \(\text{ord}_p = -\frac{1}{p-1}\), so there exists \((p-1)\) roots with \(\text{ord}_p = -\frac{1}{p-1}\). Let \( \pi_s \) be one of these, \(\text{ord}_p(\pi_s) = -\frac{1}{p-1}\). Set

\[
\theta_s(t) := E_s(\pi_s t).
\]

Note, by the above proposition \( \theta_{\infty}(t) = E(\pi_\infty t) \in L(\frac{1}{p-1}; 0) \).

**Theorem 8.6.** \( \theta_s(t) \) is a splitting function for all \( s \in \mathbb{Z}_{\geq 1} \cup \{+\infty\} \).

(the most commonly used are \( s = 1 \) and \( s = \infty \))

Side note: For \( s = 1 \), \( E_1(t) = \exp(t + \frac{t^p}{p}) \). \( \pi_1 + \pi_1^p/p = 0 \) by definition, so \( \pi_1^{p-1} = -p \). Thus, \( \theta_1(t) = E_1(\pi_1 t) = \exp(\pi_1 t + \frac{\pi_1^p}{p}) = \exp(\pi_1(t - \pi^p)) \). Claim: \( \theta_1(1) \) is a primitive \( p \)-th root of unity. Warning: \( \theta_1(1) \neq \exp(\pi_1(0)) = 1 \) is a subtle thing in \( p \)-adic analysis \((f \circ g)(a) = f(g(a)) \) if \( g(a) \notin \text{radius of convergence of } f \).

**Proof. Proof of overconvergence:** Set \( a_j := \frac{1}{p-1} - \frac{1}{p^j}(j + \frac{1}{p-1}) \). Claim: \( \theta_s(t) \in L(a_{s+1}; 0) \) (in our case: \( s = 1, \theta_1(t) \in L(\frac{1}{p-1}; 0) \) and \( s = \infty, \theta_{\infty}(t) \in L(\frac{1}{p-1}; 0) \)). To see this,

\[
\exp\left(\frac{(\pi_s t)^{p^j}}{p^j}\right) = \sum_{m=0}^{\infty} \frac{\pi_s^{p^j m}}{m! p^{jm}} t^{p^j m} \in L(a_j; 0)
\]

Since

\[
\text{ord}_p\left(\frac{\pi_s^{p^j m}}{m! p^{jm}}\right) \geq p^j m(a_j).
\]

Next, write \( \theta_s(t) = E(\pi_s t) \prod_{j \geq s+1} \exp\left(-\frac{(\pi_s t)^{p^j}}{p^j}\right) \). \( \exp\left(-\frac{(\pi_s t)^{p^j}}{p^j}\right) \in L(a_j; 0) \) so \( \prod_{j \geq s+1} \exp\left(-\frac{(\pi_s t)^{p^j}}{p^j}\right) \in L(a_{s+1}; 0) \) and \( E(\pi_s t) \in L(\frac{1}{p-1}; 0) \) by the proposition. Thus, \( \theta_s(t) \in L(a_{s+1}; 0) \).

**Proof of root of unity:** We will show next time that

\[
\text{ord}_p(\theta_s(1) - 1) = \frac{1}{p-1} (*)
\]

Suppose \((*)\) is true then we can plug it into \( \log(1 + x) \):

\[
\log(\theta_s(1)) = \sum_{j=0}^{s} \frac{\pi_s^{p^j}}{p^j} = 0
\]

Fact 1: \( \log(x) = 0 \) iff \( x \) is a primitive \( p^r \)-th root of unity for some \( r \). (pf in Koblitz p. 100, uses NP)

Hence, \( \theta_s(1) \) is a primitive \( p^r \)-th root of unity.

Fact 2: If \( \zeta \) is a primitive \( p^r \)-th root of unity then \( \text{ord}_p(1 - \zeta) = 1/p^{r-1}(p-1) \).

This implies, \( \theta_s(1) \) is a primitive \( p \)-th root of unity by \((*)\).

It remains to show \((*)\) and the splitting property. We will finish next time.
9 Lecture 7 - Malcolm

Last time: We showed if \( \theta_s(1) \) is a primitive \( p \)-th root of unity if

\[
\text{ord}_p (\theta_s(1) - 1) = \frac{1}{p-1}
\]

**Proof.** Write

\[
\theta_s(t) \cdot \prod_{j \geq s+1} \exp \left( \frac{(\pi_s t)^{p^j}}{p^j} \right) = E(\pi_s t)
\]

We then take equation (7) modulo \( t^{1+p^s+1} \) and get

\[
\theta_s(t) \cdot \left( 1 + \frac{(\pi_s t)^{p^s+1}}{p^{s+1}} \right) \equiv E(\pi_s t) \mod (t^{1+p^s+1})
\]

\[
\Rightarrow \theta_s(t) + \frac{(\pi_s t)^{p^s+1}}{p^{s+1}} - E(\pi_s t) \equiv 0 \mod (t^{1+p^s+1})
\]

(8)

Now the LHS \( \in L(a_{s+1}; 0) \) and is divisable by \( t^{1+p^s+1} \) by equation (8) and thus,

\[
\text{ord}_p \left( \theta_s(1) + \frac{(\pi_s)^{p^s+1}}{p^{s+1}} - E(\pi_s) \right) \geq a_{s+1}(1 + p^{s+1})
\]

\[
\Rightarrow \text{ord}_p \left( \theta_s(1) + \frac{(\pi_s)^{p^s+1}}{p^{s+1}} - 1 - \pi_s - \pi_s^2 C \right) \geq a_{s+1}(1 + p^{s+1})
\]

for some \( C \) with \( \text{ord}_p(C) \geq 0 \).

**Fact:** if \( \text{ord}_p(a + b) < \epsilon \) and \( \text{ord}_p(a) < \epsilon \) then \( \text{ord}_p(a) = \text{ord}_p(b) \)

We then compute:

\[
\text{ord}_p \left( \frac{(\pi_s)^{p^s+1}}{p^{s+1}} - \pi_s - \pi_s^2 C \right) = \frac{1}{p-1} < \left( \frac{p-1}{p^2} \right) (1 + p^2) \leq a_{s+1}(1 + p^{s+1})
\]

We then use the previous fact with \( a = \frac{(\pi_s)^{p^s+1}}{p^{s+1}} - \pi_s - \pi_s^2 C \) and \( b = \theta_s(1) - 1 \). Thus

\[
\text{ord}_p(b) = \text{ord}_p(\theta_s(1) - 1) = \frac{1}{p-1}
\]

**Proof of 3.** Suppose \( \hat{\nu} = \hat{t} \) is a Teich. Then

\[
\sum_{i=0}^{a-1} \hat{\nu}^i
\]

\[
\theta_s(\hat{t}) \theta_s(\hat{\nu}) \cdots \theta_s(\hat{\nu}^{n-1}) = \exp \left( \sum_{j=0}^{s} \left[ \sum_{i=0}^{a-1} \left( \hat{\nu}^i \right)^{p^j} \right] \frac{\pi_s^j}{p^j} \right) = \theta_s(1)^{\hat{t} + \hat{\nu} + \cdots + \hat{\nu}^{n-1}} = \theta_s(1)^{\text{Tr}_{\mathbb{F}^m_p / \mathbb{F}_p}(\hat{t})}
\]

where \( \hat{t} = \text{Teich}(\hat{t}) \).

**9.1 L-functions**

Let \( \psi \) be an additive character on \( \mathbb{F}_q \), \( q = p^e \). That is \( \psi \) is a group homomorphism \( \psi : (\mathbb{F}_q, +) \rightarrow (\mathbb{C}_p, \cdot) \). Let \( f \in \mathbb{F}_q[x_1^\pm, x_2^\pm, \ldots, x_n^\pm] \) be a Laurent polynomial. For each \( m \in \mathbb{Z}_{\geq 1} \), define the (toric) exponential sum

\[
S_m(f) := \sum_{x_1, \ldots, x_n \in \mathbb{F}_q^m} \psi \circ \text{Tr}_{\mathbb{F}^m_q / \mathbb{F}_q}(f(x_1, \ldots, x_n)) \in \mathbb{C}
\]

and define the \( L \)-function associated to \( S_m \) as
\[ L(f, T) := \exp \sum_{m=1}^{\infty} \frac{S_m(f) T^m}{m!} \]

We will use Dwork's trace formula to show \( L(f, T) \) is \( p \)-adic meromorphic (ie a quotient of two \( p \)-adic entire functions). It will also have a non-trivial complex radius of convergence. Thus \( L(f, T) \) is a rational function (ie a polynomial divided by a polynomial).

**Frobenius Operator**

Write \( \overline{f}(x) = \sum a_u x^u \) where \( u \in \mathbb{Z}^n, x^u = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n} \), and \( a_u \in \mathbb{F}_q \). Define \( \text{supp}(\overline{f}) := \{ u \in \mathbb{Z}^n \mid x^u \in f \} \). Let \( f(x) = \sum a_u x^u \in \mathbb{Q}_q[x_1, \ldots, x_n] \) where \( a_u = \text{Teich}(\overline{a_u}) \). Let \( \Delta(f) \) be the convex hull in \( \mathbb{R}^n \) of the origin and all the points \( u \in \text{supp}(f) \). This is called the **Newton polytope** of \( f \).

**Example 1:** Let \( f(x_1, x_2) = x_1 + x_2 + \frac{1}{x_1 x_2} \). Then \( \Delta(f) \) consists of the triangle connecting the points \((-1, -1), (1, 0), \) and \((0, 1)\) in \( \mathbb{R}^2 \).

**Example 2:** Let \( f(x_1, x_2) = x_1^3 + x_2 \). Then \( \Delta(f) \) consists of the triangle connecting the points \((0, 0), (3, 0), \) and \((0, 1)\) in \( \mathbb{R}^2 \).

**Definition 9.1.** Define the **cone** of \( \Delta \) to be the union of all rays from the origin passing through a face of \( \Delta(f) \). It is denoted \( \text{Cone}(\Delta) \). Define the monoid \( M(\Delta) := M := \mathbb{Z} \cap \text{Cone}(\Delta) \). Further define a weight function \( \omega : M \to \mathbb{Q}_{\geq 0} \) by

\[ \omega(u) := \min \{ \delta \in \mathbb{R}_{\geq 0} \mid u \in \delta \Delta(f) \text{ a dilation of } \Delta(f) \} \]

**Proposition 9.2.** \( \omega \) is essentially a norm on \( M(\Delta) \). Meaning

1. \( \omega(u) = 0 \iff u = 0 \)
2. \( \forall c \in \mathbb{Z}_{\geq 0} \implies \omega(cu) = c\omega(u) \)
3. \( \omega(u + v) \leq \omega(u) + \omega(v) \) with equality if and only if \( u \) and \( v \) are cofacial.

Let \( \ell : \sum_{i=1}^{n} b_i X_i = 1, \) \( b_i \in \mathbb{Q} \) be the equation of the hyperplane passing through a face of \( \Delta \). Then one can show that for \( u \in \text{Cone}(\ell), u = (u_1, \ldots, u_n), \) we have \( \omega(u) = \sum_{i=1}^{n} b_i u_i \). Since there are only finitely many face of \( \Delta(f) \), there must exist a \( D \in \mathbb{Z}_{\geq 1} \) such that \( \omega : M \to \frac{1}{D} \mathbb{Z}_{\geq 0} \).

## Lecture 8 - Meg

Let \( \pi = \pi_\infty \). Let \( \mathbb{Z}_q[\pi] = \text{ring of integers in } \mathbb{Q}_q(\pi) \). Define

\[ C_0 := \left\{ \sum_{u \in M(\Delta)} A_u \pi^{w(u)} x^u \mid A_u \in \mathbb{Z}_q[\pi^{1/D}] \text{ and } A_u \to 0 \text{ as } w(u) \to \infty \right\} \]

For \( \xi \in C_0, \) define \( |\xi| := \sup_{u \in M} |A_u| \).

**Proposition.** \( C_0 \) is a Banach algebra over \( \mathbb{Z}_q[\pi] \). Meaning, it is a Banach space and \( |\xi_1 \cdot \xi_2| \leq |\xi_1| \cdot |\xi_2| \).

**Proof.** Proving that \( C_0 \) is a Banach space is straightforward, so we will just prove the inequality.

Let \( \xi_1 = \sum A_u \pi^{w(u)} x^u \) and \( \xi_2 = \sum B_v \pi^{v(u)} x^v \). Compute

\[ \xi_1 \cdot \xi_2 = \sum C_r \pi^{w(r)} x^r \]

where

\[ C_r = \sum_{u+v=r, u,v \in M} A_u B_v \pi^{w(u)+w(v)-w(u+v)} \]

Then

\[ |\xi_1 \cdot \xi_2| = \sup_r |C_r| \leq \sup_r \left( \max_{w(u)+v=r} |A_u||B_v||\pi^{w(u)+v-w(u+v)}| \right) \]
Notice that \( w(u) + w(v) - w(u + v) \geq 0 \), so \( \pi^{w(u) + w(v) - w(u + v)} \leq 1 \). Plugging this into the above inequality, we get that

\[
|\xi_1 \cdot \xi_2| \leq \sup_r \left( \frac{\max_{u+v=r} |A_u||B_v|}{u+v} \right)
\]

\[
\leq |\xi_1| \cdot |\xi_2|
\]

\[\square\]

Now, set \( \theta(t) = \theta_\infty(t) = E(\pi_\infty t) \).

Fact: \( \text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) = \text{cyclic} = \{1, \tau, \tau^2, \ldots, \tau^{a-1}\} \), where for \( \alpha \in \mathbb{Z}_q \),

\( \tau(\alpha) \equiv \alpha^p \mod (p) \) and \( q = p^a \).

Here, \( \tau \) is a lift of the Frobenius map on \( \mathbb{F}_q \). Recall that for Teichmullers, \( \alpha^{q-1} = 1, \tau(\alpha) = \alpha^p \).

Set

\[
F(x) = \prod_{u \in \text{supp}(f)} \theta(a_u x^u)
\]

where \( a_u = \text{Teich}(\pi_a) \), and

\[
F_a(x) = \prod_{i=0}^{a-1} F^{\tau^i}(x^p)
\]

where \( \tau \) acts on the coefficients of \( F(x) \). Then

\[
F_a(x) = \prod_{u \in \text{supp}(f)} \theta(a_u x^u) \theta(a_u^p x^{pu}) \ldots \theta(a_u^{p^a-1} x^{(p^a-1)u})
\]

Write

\[
F(x) = \sum_{r \in M} F_r \pi^{w(r)} x^r
\]

where, from the definition, \( F_r \in \mathbb{Q}_q[\pi^{1/D}] \).

**Proposition.** \( F_r \in \mathbb{Z}_q[\pi] \) (i.e. \( \text{ord}_p(F_r) \geq 0 \))

**Proof.** Recall, \( \theta(t) \in L(\frac{1}{p-1}; 0) \), meaning \( \theta(t) = \sum_{i=0}^{\infty} \theta(t^i) \text{ with } \text{ord}_p(\theta_i) \geq \frac{1}{p-1} \), coefficients in \( \mathbb{Z}_p[\pi] \). Hence, \( F(x) \) has coefficients in \( \mathbb{Z}_q[\pi] \) (but not necessarily \( F_r \)). Now,

\[
\theta(a_u x^u) = \sum_{i \geq 0} \theta_i a_u^i x^{iu}
\]

where \( x^{iu} = x_1^{iu_1} \ldots x_n^{iu_n} \). Write \( \text{supp}(f) = \{u^{(1)}, \ldots, u^{(n)}\} \) then

\[
F(x) = \prod_{u \in \text{supp}(f)} \theta(a_u x^u)
\]

\[
= \sum_{i_1, \ldots, i_N \geq 0} \theta_{i_1} \ldots \theta_{i_N} a_{u^{(1)}}^{i_1} \ldots a_{u^{(N)}}^{i_N} x_1^{iu_1+\ldots+i_Nu_N}
\]

\[
= \sum_{r \in M} F_r \pi^{w(r)} x^r
\]

where

\[
F_r = \sum_{i_1 u^{(1)} + \ldots + i_N u^{(N)} = r} \theta_{i_1} \ldots \theta_{i_N} a_{u^{(1)}}^{i_1} \ldots a_{u^{(N)}}^{i_N} \pi^{-w(r)}
\]

Compute

\[
\text{ord}(F_r) \geq \min\{\text{ord}_p(\theta_{i_1} \ldots \theta_{i_N} a_{u^{(1)}}^{i_1} \ldots a_{u^{(N)}}^{i_N}) \pi^{-w(r)}\}
\]

Recall that \( |a_u| = 1 \) and \( \text{ord}(a_u) = 0 \). Then the above quantity is

\[
\geq \min \left\{ \frac{i_1 + \ldots + i_N}{p-1} - \frac{w(r)}{p-1} \right\}
\]

\[
\geq \min \left\{ \frac{i_1 w(u^{(1)}) + \ldots + i_N w(u^{(N)})}{p-1} - \frac{w(r)}{p-1} \right\}
\]

20
where \( F \) denotes multiplication by \( F \) and \( < \tau > = \text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) \).

**Proposition.** \( \alpha \) is well-defined.

Note: If \( \xi \in C_0, F \cdot \xi \notin C_0 \). \( F \cdot \xi \) is an element of a space similar to \( C_0 \) but without the condition that \( A_u \to 0 \).

**Proof.** Let

\[
\xi = \sum_{u \in M} A_u \pi^u x^u \in C_0
\]

Write

\[
F(x) = \sum_{v \in M} F_v \pi^v x^v
\]

where

\[
B_r = \sum_{u+v=r} A_u F_v \pi^{u+w(v)}
\]

Then, by definition

\[
\psi_p \left( \sum_{r \in M} B_r x^r \right) = \sum_{r \in M} B_{pr} x^r = \sum_{r \in M} \left( B_{pr} \pi^{-w(r)} \right) \pi^w x^r
\]

Now we need to show that \( \text{ord}_p (B_{pr} \pi^{-w(r)}) \to \infty \) as \( w(r) \to \infty \). To do this we compute

\[
B_{pr} \pi^{-w(r)} = \sum_{u+v=pr} \pi^{u+w(v)-w(r)}
\]

\[
= \sum_{u \in M} A_{pr-v} F_v \pi^{u+pr-v+w(v)-w(r)}
\]

Notice that \( \text{ord}(A_{pr-v}) \geq 0 \) by definition that that \( \text{ord}(F_v) \geq 0 \) by a previous proposition. In addition, \( w(pr-v) + w(v) - w(r) \geq pw(r) - w(v) + w(v) - w(r) = (p-1)w(r) \). From this we have that

\[
\text{ord}_p (B_{pr} \pi^{-w(r)}) \geq \text{ord}(\pi^{(p-1)w(r)})
\]

\[
= \frac{(p-1)w(r)}{p-1}
\]

\[
= w(r)
\]

\( \square \)

**Goal:** Show \( \text{Tr}(\alpha) \) makes sense. Same for \( \text{det}(1 - \alpha T) = \prod (1 - z_j T) \) and \( L(F, t) = \frac{\text{det}(1 - \alpha T)}{\text{det}(1 - q^0 T)} \).
Proof. We begin by noting that since both sides of (9) are linear expressions in $H$, it suffices to prove it for the case where $H$ is a monomial, say $H(x) = x^u$. On the right hand side of (9), we have

$$\sum_{x^{q-1} = 1} x^u = \begin{cases} (q-1)^n & \text{if } (q-1)|u \\ 0 & \text{otherwise.} \end{cases}$$

This is easy to prove: in the first case, we are simply summing $1 (q-1)^n$ times, and in the second case, multiplying by some $y^u$ with $y^q \neq 1$ shows that the sum must be zero. The details are left as an exercise.

Now, for the left hand side. First, note that the set of $x^v$ with $w(v) \leq R$ forms a basis of $W_R$. Thus, to compute the trace of $\psi_q \circ x^u$ on $W_R$, it suffices to compute $\psi_q \circ x^u(x^v)$ for each $v$ with $w(v) \leq R$. From the definitions, it is easy to see that

$$(\psi_q \circ x^u)(x^v) = \psi_q(x^{u+v}) = \begin{cases} 0 & \text{if } q \nmid u+v \\ x^{u+v} & \text{if } q|u+v. \end{cases}$$

For a basis element $x^v$ to contribute to the trace, we must have $(\psi_q \circ x^u)(x^v) = x^v$, which is only true if $\frac{u+v}{q} = v$, i.e. $v = \frac{u}{q-1}$, which implies that $(q-1)|u$. Hence

$$\text{Tr}(\psi_q \circ x^u|W_R) = \begin{cases} 0 & \text{if } (q-1) \nmid u \\ 1 & \text{if } (q-1)|u, \end{cases}$$

which concludes the proof. (note that when $R$ is sufficiently large, none of the above depends on $R$.)

Now, if $R \geq \frac{N}{q-1}$, then by a similar argument to the one that showed that $\psi_q \circ H(x)$ is an endomorphism of $W_R$, we know that $\psi_q^m \circ H(x)H(x^q)\ldots H(x^{q^{m-1}})$ is also an endomorphism of $W_R$.

Next, note that (from definitions), $\psi_q \circ H(x^q) = H(x) \circ \psi_q$. We can proceed by induction to obtain

$$\psi_q^m \circ H(x)H(x^q)\ldots H(x^{q^{m-1}}) = (\psi_q \circ H(x))^m.$$  

From this discussion and the previous theorem, we conclude

**Corollary 11.2.** $(q^m-1)^n \text{Tr}((\psi_q \circ H(x))^m|W_R) = \sum_{x^{q^m-1} = 1} H(x)H(x^q)\ldots H(x^{q^{m-1}}).$

This corollary allows us to write $S_m(\tilde{f}) = \sum_{x^{q^m-1} = 1} F_a(x)F_a(x^q)\ldots F_a(x^{q^{m-1}})$.

Let $F_{a,R}(x)$ be the sum of terms $a_u x^u$ in the expansion of $F_a$ with $w(u) \leq R$, i.e. $F_{a,R}$ is the image of $F_a$ under the canonical projection onto $W_R$. Set $a_{u,R} := \psi_q \circ F_{a,R}$, and note that this is an endomorphism of $W_R$ for $R$ sufficiently large. This implies that

$$S_m(\tilde{f}) = \lim_{R \to \infty} \sum_{x^{q^m-1} = 1} F_{a,R}(x)F_{a,R}(x^q)\ldots F_{a,R}(x^{q^{m-1}})$$

$$= \lim_{R \to \infty} (q^m-1)^n \text{Tr}((\psi_q \circ F_{a,R})^m|W_R)$$

$$= \lim_{R \to \infty} (q^m-1)^n \text{Tr}(a_{u,R}^m|W_R),$$

so that

$$L(\tilde{f}, T) = \lim_{R \to \infty} \exp \left( \sum_{m=1}^{\infty} (q^m-1)^n \text{Tr}(a_{u,R}^m) \frac{T^m}{m} \right).$$
Lemma 11.3. If $M$ is a linear transformation on a finite-dimensional vector space $V$, then

$$\exp \left( \sum_{m=1}^{\infty} \frac{\text{Tr}(M^m) T^m}{m} \right) = \det(1 - MT)^{-1}.$$ 

**Proof.** Suppose $V$ has dimension $n < \infty$. We can put $M$ in Jordan block form, with elements $b_i$ along the diagonal, so that the elements on the diagonal of $M^m$ are $b_i^m$. Thus,

$$\text{Tr}(M^m) = \sum_{i=1}^{n} b_i^m,$$

which implies

$$\exp \left( \sum_{m=1}^{\infty} \frac{\text{Tr}(M^m) T^m}{m} \right) = \prod_{i=1}^{n} \exp \left( \sum_{m=1}^{\infty} \frac{(b_i T)^m}{m} \right) = \prod_{i=1}^{n} (1 - b_i T)^{-1} = \det(1 - MT)^{-1}.$$ 

Define the Fredholm determinant of $\alpha_a$ as $\det(1 - \alpha_a T) := \lim_{R \to \infty} \det(1 - \alpha_a R T)$. Also, define the $\delta$ operator as $g(x)^\delta := \frac{g(x)}{g(qx)}$. Putting the above together with the binomial expansion for $(q^m - 1)^n$, we see that

$$L(\delta, T) = \det(1 - \alpha_a T)^\delta.$$ 

12 Lecture 10 - Brendan

12.1 The Newton Polygon of $\det(1 - \alpha_a T)$

Last time we considered operators $\alpha_a := \psi_q \circ F_a(x) : C_0 \to C_0$ and showed that

$$L(\delta, T)^{(-1)^{n+1}} = \det(1 - \alpha_a T)^\delta$$

where $\delta$ is the operator defined by $g(T)^\delta = g(T)/g(qT)$. We want to show that $\det(1 - \alpha_a T) = \sum_{m=0}^{\infty} c_m T^m$ is $p$-adic entire, and we plan to show this by showing that its Newton polygon has infinitely many pieces. In this lecture we will reduce the computation of the Newton polygon of $\det(1 - \alpha_a T)$ to the computation of the Newton polygon of a slightly less complicated determinant.

Recall that

$$\alpha := \tau^{-1} \circ \psi_p \circ F(x)$$

$$\alpha_a := \psi_q \circ F_a(x).$$

We would rather work with $\alpha$ than with $\alpha_a$. To make this reduction, we first observe that $\alpha_a = \alpha^\delta$:

$$\alpha_a = \psi_q \circ F_a$$

$$= \psi_p^\alpha \circ F^{\tau^{-1}}(x^p \tau^{-1}) \cdots F^\tau(x^p)$$

$$= (\tau^{-1} \circ \psi_p \circ F(x)) \circ \cdots \circ (\tau^{-1} \circ \psi_p \circ F(x))$$

$$= \alpha^\delta.$$

The next step in the reduction is to make a change of scalars of $C_0$. Recall that

$$C_0 = \{ \sum_{u \in M} A_u \hat{w}(u) x^u : A_u \in \mathbb{Z}_q[\hat{\pi}], A_u \to 0 \text{ as } w(u) \to \infty \}.$$ 

We can view $C_0$ as a vector space over $\mathbb{Q}_q(\hat{\pi})$ with basis $\{ x^u \}$, or we can view $C_0$ as a vector space over $\mathbb{Q}_p(\hat{\pi})$ with basis $\eta_1 x^u$, where $\eta_1, \ldots, \eta_n$ is a basis of $\mathbb{Q}_q$ over $\mathbb{Q}_p$. (In analogy to complexification, we have that $C_0/\mathbb{Q}_q = \mathbb{Q}_q \otimes_{\mathbb{Q}_q} (C_0/\mathbb{Q}_p)$.) This gives us two Fredholm determinants:

$$\det_q (1 - \alpha_a T) \quad \text{and} \quad \det_p (1 - \alpha_a T).$$
where $\det_q$ denotes the determinant over $\mathbb{Q}_q(\tilde{x})$ and $\det_p$ denotes the determinant over $\mathbb{Q}_p(\tilde{x})$. The two are related by

$$
\det_p(1 - \alpha_T) = \text{Norm}_{\mathbb{Q}_q(\tilde{x})/\mathbb{Q}_p(\tilde{x})}(\det_q(1 - \alpha_T))
$$

$$
= \prod_{i=0}^{a-1} \tau^i(\det_q(1 - \alpha_T))
$$

Using $\alpha = \alpha^\kappa$, we have

$$
\det_p(1 - \alpha_T^\kappa) = \det_p(1 - \alpha^\kappa T^\kappa) = \prod_{k=0}^{a-1} \det_p(1 - \zeta_\alpha^k \alpha T),
$$

where $\zeta_\alpha$ is a primitive $\alpha$th root of unity. Thus we have

$$
\prod_{i=0}^{a-1} \tau^i(\det_q(1 - \alpha_T^\kappa)) = \prod_{k=0}^{a-1} \det_p(1 - \zeta_\alpha^k \alpha T).
$$

We define $\ord_q(-) := \frac{1}{\kappa} \ord_p(-)$ so that $\ord_q(q) = 1$. Let $m$ be the number of reciprocal roots of $\det_q(1 - \alpha_T)$ of slope $\ord_q = s$ (hence $\ord_p = as$). We will show the following:

**Lemma 12.1.** $\det_q(1 - \alpha_T)$ has $m$ reciprocal roots of $\ord_p = as$ if and only if $\det_p(1 - \alpha_T)$ has $am$ reciprocal roots of $\ord_p = s$.

**Proof.** If $r$ is a reciprocal root of $\det_q(1 - \alpha_T)$, then $\zeta_{\alpha}^{1/\kappa}$ is a reciprocal root of $\det_q(1 - \alpha_T^\kappa)$. Hence $\det_q(1 - \alpha_T^\kappa)$ has $am$ reciprocal roots of slope $s$, which holds if and only if

$$
\prod_{i=0}^{a-1} \tau^i(\det_q(1 - \alpha_T^\kappa))
$$

has $(am)^s$ reciprocal roots of slope $\ord_p = s$. Since $\ord_p(\zeta_\alpha) = 0$, it follows that each term in the product on the right hand side of equation 10 has $am$ reciprocal roots of slope $s$, which holds if and only if $\det_p(1 - \alpha_T)$ has $am$ reciprocal roots of slope $\ord_p = s$.

This lemma lets us translate between the $q$-adic Newton polygon (using $\ord_q$) of $\det_q(1 - \alpha_T)$ and the $p$-adic Newton polygon (using $\ord_p$) of $\det_p(1 - \alpha_T)$.

**Proposition.** The $q$-adic Newton polygon of $\det_q(1 - \alpha_T)$ has vertices $(\sum_{i=1}^{\ell} m_i, \sum_{i=1}^{\ell} s_i)$ for $\ell \in \mathbb{Z}_{\geq 1}$ if and only if the $p$-adic Newton polygon of $\det_p(1 - \alpha_T)$ has vertices $(\sum_{i=1}^{\ell} a m_i, \sum_{i=1}^{\ell} a s_i)$ for $\ell \in \mathbb{Z}_{\geq 1}$.

**Proof.** Immediate from previous lemma. 

### 12.2 p-adic Directness

We will use a concept called $p$-adic directness to write $\mathbb{Q}_q(\tilde{x})$ as a direct sum of $\alpha$ copies of $\mathbb{Q}_p(\tilde{x}) (q = p^\alpha)$ in a way that gives the $p$-adic order of an element of $\mathbb{Q}_q(\tilde{x})$ in terms of its coefficients. To find a basis of $\mathbb{Q}_q(\tilde{x})$ over $\mathbb{Q}_p(\tilde{x})$ we start with a basis $\{\tilde{a}_1, \ldots, \tilde{a}_\alpha\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$ and lift it to $\mathbb{Z}_q[\tilde{x}]$. We will let $\{\eta_1, \ldots, \eta_\alpha\}$ denote such a lifting.

**Lemma 12.2 (Dwork).** The basis $\{\eta_i\}$ (as above) has the property that if $g \in \mathbb{Q}_q(\tilde{x})$ can be written as

$$
g = h_1 \eta_1 + \cdots + h_\alpha \eta_\alpha \quad h_i \in \mathbb{Q}_p(\tilde{x})
$$

then $\ord_p(g) = \min\{\ord_p(h_i)\}$.

This says that if we use the $p$-adic norm in $\mathbb{Q}_q(\tilde{x})$, then $\mathbb{Q}_q(\tilde{x}) \cong \bigoplus_{i=1}^\alpha \mathbb{Q}_p(\tilde{x})$ with the sup norm. $\mathbb{Q}_q$ is something like an $L^\infty$ direct sum of $\mathbb{Q}_p$’s.

**Proof.** We begin with some preliminaries. Recall that $\tilde{x} = \pi^{1/D}$, where $\pi = \pi_\infty$ is the root of the $\infty$ splitting function and $w : M \to \frac{1}{\pi} \mathbb{Z}_{\geq 0}$. Thus

$$
\ord_p(\tilde{x}) = \frac{1}{D} \ord_p(\pi) = \frac{1}{D(p-1)}.
$$

Also, for any $\xi \in \mathbb{Z}_q[\tilde{x}]$ we let $\tilde{\xi}$ denote the image of $\xi$ in the residue field $\mathbb{F}_q/\mathbb{F}_p$.

Without loss of generality, assume that $\ord_p(g) = 0$. Set $-c = D(p-1) \min\{\ord_p(h_i)\}$.

Suppose that $c > 0$. Then

$$
0 = (\pi^c g) = (\pi^c h_1) \tilde{\eta}_1 + \cdots + (\pi^c h_\alpha) \tilde{\eta}_\alpha.
$$

24
Since \( \{ \tilde{h}_i \} \) is a basis, the coefficients \((\pi^e \tilde{h}_i)\) are zero. This implies that \( \pi^e \tilde{h}_i \in \tilde{\pi} \mathbb{Z}_q[\tilde{\pi}] \) for \( i = 1, \ldots, a \); hence \( h_i \in \tilde{\pi}^{1-e} \mathbb{Z}_q[\tilde{\pi}] \).

Thus, for \( i = 1, \ldots, a \) we have
\[
\ord_p(h_i) \geq \ord_p(\tilde{\pi}^{1-e}) = \frac{1-c}{D(p-1)} = \frac{1}{D(p-1)} + \min_j \{ \ord_p(h_j) \},
\]
which is a contradiction since the minimum is attained for some \( j \), hence \( c \leq 0 \).

Thus \( D(p-1) \min \{ \ord_p(h_i) \} \geq 0 \), and so \( \min \{ \ord_p(h_i) \} \geq 0 = \ord_p(g) \). Since \( \ord_p(g) \geq \min \{ \ord_p(h_i) \} \) by the ultrametric triangle inequality, we have \( \ord_p(g) = \min \{ \ord_p(h_i) \} \), as desired. \( \square \)

12.3 Side Note

This is something we should have done before. (So hopefully we’ll fix it in editing ;)

In showing that \( \alpha = \tau^{-1} \circ \psi \circ F : C_0 \to C_0 \) is well defined, we showed the following. Write
\[
F(x) = \sum_{v \in M} F'_v . x^v .
\]
In the original definition, we wrote \( F_{u}w(u) \) instead of \( F'_v \). Then
\[
\alpha(x^u) = \tau^{-1} \circ \psi \circ F(x) \cdot x^u
\]
\[
= \tau^{-1} \circ \psi \left( \sum_{v \in M} F'_v x^{v+u} \right)
\]
\[
= \tau^{-1} \circ \psi \left( \sum_{v \in M} F'^{pr-u} x^v \right)
\]
\[
= \tau^{-1} \left( \sum_{v \in M} F'^{pr-u} x^v \right)
\]
\[
= \sum_{v \in M} (F'^{pr-u})^{-1} x^v,
\]
and from Meg’s notes
\[
\ord_p\left( (F'^{pr-u})^{-1} \right) \geq \frac{pw(r) - w(u)}{p-1}.
\]

13 Lecture 11 - Siegfried

Denote \( \tilde{\pi} := \pi^{1/D} \), where \( \pi = \pi_{\infty} \) and the weight function \( w \) from \( M := M(\Delta) \) has image \( \frac{1}{D} \mathbb{Z}_{\geq 0} \). The goal in this lecture is to get a lower bound for the Newton polygon of \( \det_{Q_p(\tilde{\pi})} (1 - \alpha T) \), where \( \alpha := \tau^{-1} \circ \psi \circ F(x) \). An orthonormal basis\(^2\) of

\[
C_0 := \left\{ \sum_{u \in M} A_u \pi^w(u) x^u \bigg| A_u \in \mathbb{Z}_q[\tilde{\pi}], A_u \to 0 \text{ as } w(u) \to \infty \right\}
\]
as a Banach algebra\(^3\) over \( \mathbb{Z}_q[\tilde{\pi}] \) is \( B := \{ x^u | u \in M \} \) and an orthonormal basis for \( C_0 \) over \( \mathbb{Z}_p[\tilde{\pi}] \) is \( B^\prime := \{ \eta_i x^u | u \in M, 1 \leq i \leq a \} \), where \( \{ \eta_1, \ldots, \eta_a \} \) is a lifting\(^4\) of a basis of \( F_q/F_p \) into \( \mathbb{Z}_q[\tilde{\pi}] \) so that it is a basis for \( Q_q(\tilde{\pi}) \) over \( Q_p(\tilde{\pi}) \). The action of \( \alpha \) on \( B^\prime \) is given by, using its definition,
\[
\alpha(\eta_i x^u) = \tau^{-1} \circ \psi \circ F(x) (\eta_i x^u)
\]
\[
= \tau^{-1} \left( \eta_i \psi_p(F(x) x^u) \right)
\]
\[
= \tau^{-1} (\eta_i) \cdot \left( \tau^{-1} \circ \psi_p(F(x) x^u) \right)
\]
\[
= \tau^{-1} (\eta_i) \cdot \sum_{v \in M} (u; v)x^v, \quad \text{say}.
\]


\(^3\)It was proved in the 03Oct lecture that \( C_0 \) is a Banach algebra over \( \mathbb{Z}_q[\tilde{\pi}] \).

\(^4\)by taking Teichmüller representatives of any basis of \( F_q/F_p \); the lifting is basis of \( Q_q(\tilde{\pi}) \) over \( Q_p(\tilde{\pi}) \) since it has \( a \) elements and is linearly independent by the following argument: Let \( \eta_{\tilde{\eta}_1}, \ldots, \eta_{\tilde{\eta}_a} \) be a basis for \( F_q/F_p \). If \( \eta_{\tilde{\eta}_1}, \ldots, \eta_{\tilde{\eta}_a} \) are linearly dependent in \( Q_q(\tilde{\pi}) \) then there is a linear combination \( b_1 \eta_{\tilde{\eta}_1} + \cdots + b_a \eta_{\tilde{\eta}_a} = 0 \) with \( b_j \)'s in \( Q_p(\tilde{\pi}) \) not all zero. Multiply through by \( \pi^k \) with \( k \) the least integer that makes each \( \pi^k b_j \) have nonnegative \( \ord_p \), so that at least one of them have \( \ord_p \) exactly zero. Reduce the resulting equation mod \( p \) to get an equation of linear dependence of \( \eta_{\tilde{\eta}_1}, \ldots, \eta_{\tilde{\eta}_a} \) in \( F_q \), contradicting the fact that they form a basis.
If \( F(x) = \sum_{r \in M} F_r x^r \), then the determinant of its infinite matrix \( F \) is given by \( \det_F = \prod_{\ell} D(i, u; \ell; \xi \ell, \eta \ell) \) for each \( \ell \) with \( F \). Write \( c(u; v) = \sum_{j=1}^a c(u; v) j \eta_j \), with \( c(u; v) j \in \mathbb{Z}_p[\tilde{\pi}] \) for each \( j \). By Dwork’s lemma of \( p \)-adic directness, \( \min_j \operatorname{ord}_p(c(u; v) j) = \operatorname{ord}_p(c(u; v)) \), so
\[
\operatorname{ord}_p(c(u; v) j) \geq \frac{\min\{\operatorname{ord}_p(c(u; v) j)\}}{p - 1} = \operatorname{ord}_p(c(u; v)) \]
for each \( j \).

Now write \( \tau^{-1}(\eta_i) \eta_j = \sum_{s=1}^a b(i, j, s) \eta_s \), with \( b(i, j, s) \in \mathbb{Z}_p[\tilde{\pi}] \). Then the above expression for \( \alpha(\eta_i x^u) \) becomes
\[
\alpha(\eta_i x^u) = \tau^{-1}(\eta_i) \cdot \sum_{u \in M} \sum_{j=1}^a c(u; v) j \eta_j x^v
= \sum_{u \in M} \sum_{s=1}^a c(u; v) j b(i, j, s) \eta_s x^v
= \sum_{u \in M} D(i, u; v) \eta_s x^v, \quad \text{say.}
\]

Hence the (infinite) matrix of \( \alpha \) with respect to the basis \( B' \) is given by
\[
\alpha = (\alpha(s, v), (i, u)) = (D(i, u; v)) \quad \eta_s x^v \in B'.
\]

Note that, since each \( b(i, j, s) \) has nonnegative \( \operatorname{ord}_p \), the ultrametric inequality gives
\[
\operatorname{ord}_p(D(i, u; v)) \geq \min_{1 \leq j \leq a} \{ \operatorname{ord}_p(c(u; v) j b(i, j, s)) \}
\geq \min_{1 \leq j \leq a} \operatorname{ord}_p(c(u; v) j)
\geq \max \left\{ 0, \frac{pw(v) - w(u)}{p - 1} \right\}
\]
from the above. Write
\[
\det_{\mathbb{Q}_p[\pi]}(1 - \alpha T) = \sum_{m=0}^{\infty} c_m T^m.
\]
Then by a general formula for the determinant of an infinite matrix
\[
c_m = (-1)^m \sum_{\ell=1}^{\infty} \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{m} D(i, u; i, u) = (-1)^m \sum_{\ell=1}^{\infty} \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{m} D(i, u; i, u).
\]

---

5. This was computed in the 03Oct lecture.
6. This was computed in the 15Oct lecture.
7. Using that \( \eta_1, \ldots, \eta_a \) is a basis, we only know at first that the \( c(u; v) j \) are in \( \mathbb{Q}_p[\pi] \), but the argument that follows (using \( p \)-adic directness) shows that they are in \( \mathbb{Z}_p[\tilde{\pi}] \).
8. From the 15October lecture.
9. The same reasoning as for \( c(u; v) \) gives that each \( b(i, j, s) \) is in \( \mathbb{Z}_p[\tilde{\pi}] \). Recall that Teichmüller representatives have \( \operatorname{ord}_p \) exactly 0. Note that, since \( \tau \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p) \) and \( \tau \) preserves the norm, we have \( \tau^{-1}(\eta_i) \in \mathbb{Z}_p[\tilde{\pi}] \) for each \( i \), but as far as we know, they may not be in \( \mathbb{Z}_p[\pi] \) because they may not be in \( \mathbb{Z}_p[\tilde{\pi}] \).
10. For the general formula, see §5 of Serre: Completely Continuous Endomorphisms of \( p \)-adic Banach Spaces. To show that the expression for \( c_m \) converges, observe that the \( \operatorname{ord}_p \) of each term is nonnegative by the lower bound for \( \operatorname{ord}_p(D(i, u; v)) \). If we take the identity \( \sigma \), then \( \operatorname{ord}_p(\prod_{\ell=1}^{m} D(i, u; i, u)) \) is equal to the sum of the \( \operatorname{ord}_p \)s of the factors, each of which is \( \geq \frac{pw(u_{x^v}) - w(u_{x^v})}{p - 1} = w(u_{x^v}) \). Thus \( \operatorname{ord}_p(\prod_{\ell=1}^{m} D(i, u; i, u)) \) goes to infinity as the largest \( w(u_{x^v}) \) of the powers \( u_{x^v} \) in \( E_m \) goes to infinity.
where $\mathcal{E}_m$ is the set of all subsets of $B'$ with $m$ elements and $S_m$ is the group of permutations of $\{1, \ldots, m\}$. Now the ultrametric inequality\(^{11}\) gives

$$\text{ord}_p(c_m) \geq \min_{\ell \in \mathcal{E}_m} \min_{\sigma \in S_m} \sum_{\ell=1}^{m} \text{ord}_p(D(i\ell, u_\ell; i\sigma(\ell), u\sigma(\ell)))$$

$$\geq \min_{\ell \in \mathcal{E}_m} \min_{\sigma \in S_m} \left( \sum_{\ell=1}^{m} \frac{pw(u_\sigma(\ell)) - w(u_\ell)}{p-1} \right)$$

$$= \min_{\ell \in \mathcal{E}_m} \min_{\sigma \in S_m} \left( \frac{p}{p-1} \sum_{\ell=1}^{m} w(u_\sigma(\ell)) - \frac{1}{p-1} \sum_{\ell=1}^{m} w(u_\ell) \right)$$

$$= \min_{\ell \in \mathcal{E}_m} \sum_{\ell=1}^{m} w(u_\ell) \text{ because the two sums are equal since } \sigma \text{ is a permutation}$$

$$= \min_{\ell \in \mathcal{E}_m} \sum_{\ell=1}^{m} w(u_\ell).$$

Now there are only finitely many lattice point $u$'s with small $w(u)$. This suggests defining for each nonnegative integer $N$ the nonnegative integer

$$W(N) := \# \left\{ u \in M \mid w(u) = \frac{N}{D} \right\}.$$

Note that\(^{12}\) $W(N) \to \infty$ as $N \to \infty$. Since there are $a$ many $\eta_j$'s, there are exactly $aW(N)$ elements $\eta_jx^n$ in the basis $B'$ that have $w(u) = N/D$. If $m$ is a positive integer, then\(^{13}\)

$$m = \sum_{N=0}^{R-1} aW(N) + \rho$$

for some integer $R \geq 0$ and integer $\rho$ with $0 \leq \rho < aW(R)$. Hence

$$\text{ord}_p(c_m) \geq \min_{\ell \in \mathcal{E}_m} \sum_{\ell=1}^{m} w(u_\ell)$$

$$= \sum_{N=0}^{R-1} aW(N) \cdot \frac{N}{D} + \rho \cdot \frac{R}{D}$$

by choosing $\mathcal{E}_m$ to be made up of the first $m$ elements in $B'$ if the elements in $B'$ are arranged in increasing $w(u)$. Denote

$$P_R := \left( \sum_{N=0}^{R} aW(N), \sum_{N=0}^{R} aW(N) \cdot \frac{N}{D} \right)$$

for $R \geq 0$ and let $P_{-1}$ denote the origin. For $0 \leq \rho < aW(R)$, the point

$$\left( \sum_{N=0}^{R-1} aW(N) + \rho, \sum_{N=0}^{R-1} aW(N) \cdot \frac{N}{D} + \rho \cdot \frac{R}{D} \right)$$

lies on the line segment connecting the two points $P_{R-1}$ and $P_R$. Thus all the points $(m, \text{ord}_p(c_m))$ determining the Newton Polygon of $\det_{q_\alpha(\xi)}(1 - \alpha T)$ are above the line segments connecting the points $P_R$, $R = -1, 0, 1, \ldots$. Hence the $p$-adic Newton polygon of $\det_{q_\alpha(\xi)}(1 - \alpha T)$ lies above the lower convex hull of the points $P_R$, $R = -1, 0, 1, \ldots$. Thus, by a previous proposition\(^{14}\), the $q$-adic Newton polygon of $\det_{q_\alpha(\xi)}(1 - \alpha T)$ lies above the lower convex hull of the points

$$Q_R := \left( \sum_{N=0}^{R} W(N), \sum_{N=0}^{R} W(N) \cdot \frac{N}{D} \right), \quad R = -1, 0, 1, \ldots.$$

An immediate corollary to this is

\(^{11}\)or rather the version for infinite sums
\(^{12}\)That $W(N) \to \infty$ needs the assumption that the smallest dimension $\tilde{n}$ of a subspace of Euclidean space containing $\Delta$ has $\tilde{n} > 1$. For $\tilde{n} > 1$, $W(N) \to \infty$ will follow from the polynomial expansion $\sum_{j \leq D_{\xi}} W(j) = \text{vol}(\Delta)x^{\tilde{n}} + O(x^{\tilde{n}-1})$ that will be proved in a succeeding lecture. For the results in this lecture, we will only need that $W(N)$ is positive for all large $N$, which is true for any $\tilde{n} > 0$.
\(^{13}\)A sum $\sum_{N=1}^{L} a$ means $0$.
\(^{14}\)from the 15 Oct Lecture
Corollary. \( \det_{\mathbb{Q}_p}(1 - \alpha_T) \) is \( p \)-adic entire.

**Proof.** The line segments in the lower convex hull of the points \( Q_R \) are precisely the line segments connecting the points, and their slopes are \( R/D \) for those \( R \) with \( W(R) \) positive. Thus, since \( W(N) \) is positive for all large \( N \), it follows that the slopes tend to infinity as \( R \to \infty \). Hence, since the \( q \)-adic Newton polygon of \( \det_{\mathbb{Q}_p}(1 - \alpha_T) \) lies above the lower convex hull of the points \( Q_R \), it follows from a previous proposition\(^{15}\) that \( \det_{\mathbb{Q}_p}(1 - \alpha_T) \) is \( p \)-adic entire.

This immediately implies

**Corollary.** \( L(\overline{f}, T) \) is \( p \)-adic meromorphic.

**Proof.**

\[
L(\overline{f}, T)^{(-1)^{n+1}} = \det_{\mathbb{Q}_p}(1 - \alpha_T)^{\delta^n},
\]

which, when written out using the definition of \( \delta \), is a ratio of products of \( p \)-adic entire functions.

To show that \( L(\overline{f}, T) \) is in fact rational, we use the following theorem\(^{16}\).

**Theorem (Dwork-Borel).** Let the field \( E \) be a finite extension of \( \mathbb{Q} \), and let \( f \in E[[T]] \). Suppose that

1. \( f \) is \( p \)-adic meromorphic;

2. \( f \) has a positive radius of convergence in \( \mathbb{C} \).

Then \( f \in E(T) \), i.e. \( f \) is a rational function.

**Theorem.** \( L(\overline{f}, T) \in \mathbb{Q}(\zeta_p)(T) \)

**Proof.** The above corollary gives that \( L(\overline{f}, T) \) is \( p \)-adic meromorphic. To show that it is analytic at 0 in \( \mathbb{C} \), it suffices to show that the series \( \sum_{m=1}^{\infty} S_m \frac{T^m}{m} \) in the definition\(^{17}\) of \( L(\overline{f}, T) \) is complex analytic in a neighborhood of 0 in \( \mathbb{C} \). In this proof let \( | \cdot | \) mean the usual modulus \( | \cdot |_\mathbb{C} \) in \( \mathbb{C} \). Now

\[
S_m = \sum_{x_1, \ldots, x_n \in \mathbb{F}_q^\times} \Psi \circ \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\overline{f}(x_1, \ldots, x_n)),
\]

with \( \Psi : \mathbb{F}_q \to \mathbb{Q}_p(\pi) \) the additive character \( \overline{b} \mapsto \theta(1)^{\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b)} \). Since \( \theta(1) = \zeta_p \) is a primitive \( p \)-th root of unity\(^{18}\), it follows that \( |\Psi(\overline{b})|_p = 1 \) for all \( \overline{b} \) in \( \mathbb{F}_q \). Thus \( |S_m| \) is less than or equal to the number of \( n \)-tuples \( x_1, \ldots, x_n \) of elements from \( \mathbb{F}_q^\times \), and there are \( (q^m - 1)^n \) such \( n \)-tuples. Thus, for \( |T| \leq q^{-n-1} \), we have

\[
\sum_{m=1}^{\infty} S_m \frac{T^m}{m} \leq \sum_{m=1}^{\infty} |S_m| |T|^m \leq \sum_{m=1}^{\infty} q^{mn} q^{-(n+1)m} = \sum_{m=1}^{\infty} q^{-m} = \frac{1}{q-1} < \infty.
\]

Since the images of \( \Psi \) are \( p \)-th roots of unity, it follows that \( S_m \in \mathbb{Q}(\zeta_p) \) for each \( m \), and so the power series expansion for \( L(\overline{f}, T) \) around \( T = 0 \) has coefficients in \( \mathbb{Q}(\zeta_p) \), and the above theorem gives that \( L(\overline{f}, T) \) is in \( \mathbb{Q}(\zeta_p)(T) \). \( \square \)

### 14 Lecture 12 - Jamie

Recall,

\[
L(\overline{f}, T)^{(-1)^{n+1}} = \det(1 - \alpha T)^{\delta^n} = \frac{\prod_{i=1}^{R}(1 - \omega_i T)}{\prod_{j=1}^{R}(1 - \eta_j T)},
\]

where \( \delta : g(x) \mapsto \frac{g(x)}{g(qx)} \).

Set \( \Phi : g(x) \mapsto g(qx) \). Then \( \delta = 1 - \Phi \) and \( g(x)^{\delta} = g(x)^{1-\Phi} = \frac{g(x)}{g(x)^\Phi} = g(x)^{\frac{1}{\Phi(q)}} \).

\[
\det(1 - \alpha T)^{\delta^n} = \det(1 - \alpha T)^{1-\Phi} \implies \det(1 - \alpha T) = \left( \frac{\prod_{i=1}^{R}(1 - \omega_i T)}{\prod_{j=1}^{R}(1 - \eta_j T)} \right)^{1/(1-\Phi)^n}
\]

Use

\[
\frac{1}{(1-x)^n} = \sum_{m=0}^{\infty} c(m)x^m
\]

\(^{15}\)from the 19Sept lecture; the proof also works with \( \text{ord}_{q} = \frac{1}{n}\text{ord}_{p} \) in place of \( \text{ord}_{p} \)

\(^{16}\)The proof was not discussed in class; for Dwork’s proof see Theorem 2 of Dwork, B., On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.,* 82 (1960), 631-648.

\(^{17}\)as defined in the 10Oct lecture

\(^{18}\)This was proved in the 26Sept lecture.
where \( c(m) = \binom{n+m-1}{m} \). Then

\[
\det(1 - \alpha T) = \left( \frac{\prod_{i=1}^{R} (1 - \omega_i T)}{\prod_{j=1}^{S} (1 - \eta_j T)} \right)^{\sum_{m=0}^{\infty} c(m) \Phi^m}
\]

This motivates the definitions:

\[
D_1(T) := \prod_{i=1}^{R} \prod_{m=0}^{\infty} (1 - q^m \omega_i T)^{c(m)} \quad \text{and} \quad D_2(T) := \prod_{j=1}^{S} \prod_{m=0}^{\infty} (1 - q^m \eta_j T)^{c(m)}
\]

We get \( \det(1 - \alpha T) = \frac{D_1(T)}{D_2(T)} \). We have shown that this is entire. Also note, \( D_1, D_2 \) are entire. Thus, \( D_2 \mid D_1 \). Which implies \( \forall j, \eta_j = q^m \omega_i \) for some \( m \in \mathbb{Z}_{\geq 0} \) and some \( \omega_i \).

**Estimate Degree:** \( R - S \)

**Proposition 14.1. (Y-intercept method)** Let \( f(T) \in 1 + T \mathbb{C}_p[[T]] \) be entire. Write \( f(T) = 1 + \sum d_m T^m = \prod_{i=1}^{\infty} (1 - \rho_i T) \). Then \( \forall x \in \mathbb{R} \) (slopes),

\[
\sum_{x \geq \ord_q(\rho_i)} (x - \ord_q(\rho_i)) = \max \left\{ xm - \ord_q(d_m) \right\}_{m \geq 0}.
\]

**Proof.** We will show

\[
\sum (-x + \ord_q(\rho_i)) = \min(-xm + \ord_q(d_m))
\]

On the graph of the Newton polygon of \( f(T) \) graph lines with slope \( x \) going through the vertices. The parallel lines are all of the form

\[
Y - \ord_q(d_m) = x - (X - m)
\]

so they have \( Y \)-intercepts: \( -xm + \ord_q(d_m) \) the smallest such \( Y \)-intercept is \( \min(-xm + \ord_q(d_m)) \).

![Graph showing Y-intercepts and Newton polygon](image)

Viewing the same NP in terms of the \( \rho_i \):
the above line with the smallest Y-intercept has equation

\[ Y - \sum_{\text{ord}_p(\rho_i) \leq x} \text{ord}_q(\rho_i) = x(X - \sum_{\text{ord}_p(\rho_i) \leq x} 1) \]

which has Y-intercept \( \sum(-x + \text{ord}_p(\rho_i)) \). This is the same Y-intercept as before so we get the desired equality.

For us this means, since \( \det(1 - \alpha T) = \frac{D_1(T)}{D_2(T)} \), that writing \( \det(1 - \alpha T) = \sum_{m=0}^{\infty} a_m T \), the Y-intercept method gives

\[
\sum_{i=1}^{R} \sum_{\text{ord}_q(q^m \omega_i) \leq x} c(m)(x - \text{ord}_q(q^m \omega_i)) - \sum_{j=1}^{S} \sum_{\text{ord}_q(q^m \eta_j) \leq x} c(m)(x - \text{ord}_q(q^m \eta_j)) = \max_{m \geq 0} (x m - \text{ord}_q(a_m)) \tag{11}
\]

In the past we showed the NP of \( \det(1 - \alpha T) \) has as a lower bound the polygon with vertices \( (\sum_{j=0}^{r} w(j), \frac{1}{D} \sum_{j=0}^{r} j w(j)) \). If we draw lines of slope \( x \) through the vertices of this polygon these lines have Y-intercepts \( -x \sum_{j=0}^{r} w(j) + \frac{1}{D} \sum_{j=0}^{r} j w(j) \).

Thus, \( \min(-x m + \text{ord}_q(a_m)) \geq \min(-x \sum_{j=0}^{r} w(j) + \frac{1}{D} \sum_{j=0}^{r} j w(j)) \).

Hence, the right hand side of equation 11 is

\[
\max_{m \geq 0} (x m - \text{ord}_q(a_m)) \leq \max_r \left( -x \sum_{j=0}^{r} w(j) + \frac{1}{D} \sum_{j=0}^{r} j w(j) \right) = \max_r \left( \frac{1}{D} \sum_{j=0}^{r} (Dx - j) w(j) \right) = \frac{1}{D} \sum_{j \in Z_{\geq 0}, j \leq Dx} (Dx - j) w(j)
\]

For any \( x \), recall

\[
\sum_{m=1}^{x} m^n = \frac{1}{n + 1} x^{n+1} + O(x^n)
\]

Also note,

\[ c(m) = \binom{n + m - 1}{m} = \frac{1}{(n-1)!}(n + m - 1) \ldots (m + 1) = \frac{m^{n-1}}{(n-1)!} + O(m^{n-2}) \]
Since, \( \text{ord}_q(q^m \omega_i) = m + \text{ord}_q(\omega_i) \), we have,

\[
\sum_{\text{ord}_q(q^m \omega_i) \leq x} (x - \text{ord}_q(q^m \omega_i))c(m) = \sum_{m \leq x - \text{ord}_q(\omega_i)} (x - m - \text{ord}_q(\omega_i))c(m)
\]

\[
= \frac{1}{(n-1)!} \sum_{m \leq x - \text{ord}_q(\omega_i)} (xm^{n-1} - m^n + Cm^{n-1} + O(m^{n-2})
\]

\[
= \frac{1}{(n-1)!} (\frac{x^{n+1}}{n} - \frac{x^{n+1}}{n+1} + O(x^n)
\]

\[
= \frac{x^{n+1}}{n+1} + O(x^n)
\]

15 Lecture 13 - Malcolm

From last time we showed for each \( \bar{\text{Γ}} \),

\[
\sum_{\text{ord}_q(q^m \omega_i) \leq x} (x - \text{ord}_q(q^m \omega_i))c(m) = \frac{x^{n+1}}{(n+1)!} + O(x^n). \quad (12)
\]

We also have

\[
\sum_{\text{ord}_q(q^m \omega_i) \leq x} (x - \text{ord}_q(q^m \omega_i))c(m) - \sum_{j=1}^{S} \sum_{\text{ord}_q(q^m \eta_j) \leq x} (x - \text{ord}_q(q^m \eta_j))c(m) \leq
\]

is less than or equal to

\[
\leq \frac{1}{D} \sum_{j \leq Dx} (Dx - j)w(j). \quad (14)
\]

Thus using equation (12) we get

\[
(13) = \sum_{i=1}^{R} \frac{x^{n+1}}{(n+1)!} - \sum_{j=1}^{S} \frac{x^{n+1}}{(n+1)!} + O(x^n) = \frac{(R-S)}{(n+1)!} x^{n+1} + O(x^n) \leq (14).
\]

We now want to estimate equation (14).

15.1 Ehrart Theory

Recall, associated to \( \tilde{f}(x) = \sum a_u x^u, u \in \mathbb{Z}^n \) is \( \Delta(\tilde{f}) \) the Newton Polytope. That is \( \Delta(\tilde{f}) \) is the convex hull of the origin and \( \{u\} \). We say a face \( \Gamma \) of \( \Delta \) is a closed face of arbitrary dimension. For each \( \Gamma \) not containing the origin let \( C(\Gamma) \) be the union of rays from the origin passing through \( \Gamma \) and let \( M(\Gamma) = \mathbb{Z}^n \cap C(\Gamma) \). We also define \( \hat{\Gamma} \) to be the convex hull of \( \Gamma \) together with the origin. Let \( \text{vol}(\Gamma) \) be the volume of \( \Gamma \) with respect to the Haar measure of the smallest affine space containing \( \Gamma \) and such that it is normalized so that a fundamental domain induced by the lattice has volume 1. Next set \( \hat{n} \) be the dimension of the smallest subspace of \( \mathbb{R}^n \) containing \( \Delta \). For each face \( \Gamma \) define \( w_{\Gamma}(N) := \# \{ u \in M(\Gamma) | w(u) = \frac{N}{D} \} \).

Note: It may happen that \( \text{Im}(w|_{M(\Gamma)}) \) is a submonoid of \( \frac{1}{D} \mathbb{Z}_{\geq 0} \). In this case \( \text{Im}(w|_{M(\Gamma)}) = \frac{1}{D(\Gamma)} \mathbb{Z}_{\geq 0} \) where \( D(\Gamma) | D \). Thus

\[
\hat{n}(N) = 0 \quad \text{if} \quad \frac{N}{D} \neq \frac{N'}{D} \quad (\forall) N' \in \mathbb{Z}_{\geq 0}.
\]

Now consider \( N' = \frac{D(\Gamma)N}{D} \in \mathbb{Z} \) as \( N \) varies. Then

\[
\hat{n}(N) = \# \left\{ u \in M(\Gamma) | w(u) = \frac{N}{D(\Gamma)} \right\}.
\]

Let \( d(\Gamma) \) be the dimension of \( \Gamma \).

**Theorem 15.1.** \( \hat{n}(N) \) is a polynomial of degree \( d(\Gamma) \) in \( N' \) and

\[
\hat{n}(N) = \text{vol}(\Gamma) \left( \frac{N'}{D(\Gamma)} \right)^{d(\Gamma)} + \cdots \text{(lower in } N')
\]
Remember we seek to estimate (14). We do this by breaking it up as

\[(14) = x \sum_{j \leq D_x} w(j) - \frac{1}{D} \sum_{j \leq D_x} jw(j).\]

We now use a change of variables \(j = \frac{j'D}{D(\Gamma)}\) and get

\[
\sum_{j \leq D_x} w_T(j) = \sum_{j' \leq D(\Gamma)x} w_T(j) \\
= \sum_{j' \leq D(\Gamma)x} \frac{\text{vol}(\Gamma)}{D(\Gamma)d(\Gamma)} (j')^{d(\Gamma)} + \cdots \text{lower in } j' \\
= \frac{\text{vol}(\Gamma)}{D(\Gamma)d(\Gamma)} (D(\Gamma)x)^{d(\Gamma)+1} + \cdots \text{lower in } x \\
= \frac{\text{vol}(\Gamma)D(\Gamma)}{d(\Gamma)+1} x^{d(\Gamma)+1} + \cdots \text{lower in } x
\]

This means we should only consider the top dimensional \(\Gamma\) since they produce the largest growth in \(x^{d(\Gamma)+1}\). Note: The top dimensional \(\Gamma\) are \(d(\Gamma) = \tilde{n} - 1\). Thus

\[
\sum_{j \leq D_x} w_T(j) = \frac{\text{vol}(\Gamma)D(\Gamma)}{\tilde{n}} x^{\tilde{n}} + \cdots \text{lower in } x
\]

**Proposition 15.2.**

\[
\text{vol}(\hat{\Gamma}) = \frac{\text{vol}(\Gamma)D(\Gamma)}{\tilde{n}}
\]

**Proof.**

\[
\sum_{j' \leq D(\Gamma)x} w_T(j) = \#\{u \in M(\hat{\gamma}) | w(u) \leq x\} \\
= \#\{M(\hat{\Gamma}) \cap (x\hat{\Gamma})\} \\
= \text{vol}(\hat{\Gamma}) x^{d(\hat{\Gamma})} + \cdots \text{lower in } x \\
= \text{vol}(\hat{\Gamma}) x^{\tilde{n}} + \cdots \text{lower in } x.
\]

Now

\[
w(N) = \# \left\{ u \in M(\Delta) | w(u) = \frac{N}{D} \right\} \\
= \sum_{d(\Gamma) = \tilde{n}-1} w_T(N) - \sum_{d(\Gamma) = \tilde{n}-2} w_T(N) + \cdots \text{ (inclusion / exclusion)}
\]

and thus,

\[
\sum_{j \leq D_x} w(j) = \sum_{j \leq D_x} \sum_{d(\Gamma) = \tilde{n}-1} w_T(j) + \text{lower } d(\Gamma) \\
= \sum_{d(\Gamma) = \tilde{n}-1} \text{vol}(\hat{\Gamma}) x^{\tilde{n}} + \cdots \text{lower in } x
\]

and thus,

\[
= \text{vol}(\Delta) x^{\tilde{n}} + \cdots \text{lower in } x
\]
Lecture 14 - Meg

We would like to estimate

\[ \sum_{j \leq D} j w(j) \]

Letting \( j = \frac{D j'}{D(\Gamma)} \),

\[ \sum_{j \leq D} j w(j) = \sum_{\dim(\Gamma) = \tilde{n} - 1} \sum_{j' \leq D(\Gamma)} \left( \frac{D j'}{D(\Gamma)} \right) w_{\Gamma}(j) \] - (terms in \( \dim(\Gamma) < \tilde{n} - 1 \))

\[ = \sum_{\Gamma} \sum_{j'} \left( \frac{D \text{vol}(\Gamma)}{D(\Gamma)^{\tilde{n}}} (j')^{\tilde{n}} + \text{lower in } j' \right) \] - (lower in dim.)

\[ = \sum_{\Gamma} \left( \frac{D \text{vol}(\Gamma)}{D(\Gamma)^{\tilde{n}}} (D(\Gamma)x)^{\tilde{n} + 1} \right) + \text{lower in } x \]

\[ = \sum_{\dim(\Gamma) = \tilde{n} - 1} D \text{vol}(\Gamma) \frac{D(\Gamma)}{\tilde{n} + 1} x^{\tilde{n} + 1} \] + (lower in \( x \))

Now recalling that

\[ \frac{D(\Gamma) \text{vol}(\Gamma)}{\tilde{n}} = \text{vol}(\hat{\Gamma}) \]

we can simplify the above expression to

\[ \sum_{\Gamma} D \text{vol}(\hat{\Gamma}) \frac{x^{\tilde{n} + 1}}{\tilde{n} + 1} \] + (lower in \( x \))

Using the fact that

\[ \sum_{\Gamma} \text{vol}(\hat{\Gamma}) = \text{vol}(\Delta) \]

we can again simplify to get

\[ \frac{D \text{vol}(\Delta) \tilde{n}}{\tilde{n} + 1} x^{\tilde{n} + 1} \] + (lower in \( x \))

Recall why we are doing all of this. We know that

\[ L(\bar{\Gamma}, T)^{(1)} = \prod_{i=1}^{n} (1 - w_i T) \]

\[ \prod_{j=1}^{n} (1 - \eta_j T) \]

and we want to know (or at least get an estimate of) the degree of \( R - S \). So far we know that

\[ \frac{(R - S)}{(n + 1)!} x^{n + 1} \] + (lower in \( x \)) \leq \frac{1}{D} \sum_{j \leq D} (Dx - j) w(j)

\[ = x \sum_{j \leq D} w(j) - \frac{1}{D} \sum_{j \leq D} j w(j) \]

\[ = \text{vol}(\Delta) x^{\tilde{n} + 1} - \frac{\text{vol}(\Delta) \tilde{n}}{\tilde{n} + 1} x^{\tilde{n} + 1} \] + (lower in \( x \))

\[ = \frac{\text{vol}(\Delta)}{\tilde{n} + 1} x^{\tilde{n} + 1} \] + (lower in \( x \))

This estimate holds for all \( x >> 0 \).

We also know \( \tilde{n} \leq n \) since \( \Delta \subseteq \mathbb{R}^n \). If \( \tilde{n} < n \), then \( R = S \).

Now suppose that \( \tilde{n} = n \). Then \( 0 \leq R - S \leq n! \text{vol}(\Delta) \in \mathbb{Z}_{\geq 1} \). (We will show \( 0 \leq R - S \) later.) Since \( n = \tilde{n} \), \( \text{vol}(\Delta) = \text{Lebesgue volume of } \Delta \text{ in } \mathbb{R}^n \).

Note: If \( \dim(\Delta) = \tilde{n} < n \), then \( \text{vol}(\Delta) = 0 \) in Lebesgue sense. Hence the estimate \( 0 \leq R - S \leq n! \text{vol}(\Delta) \) is always
true, for \( n = \tilde{n} \) or not.

Summarizing, so far we know that given \( \overline{f} \in \mathbb{F}_q[x_1^\pm, \ldots, x_n^\pm] \Rightarrow \triangle(\overline{f}) \Rightarrow \deg L(\overline{f}, T)^{(-1)^{n+1}} \leq n! \text{vol}(\triangle) \).

Now we will fix \( \triangle_0 \) that contains the origin and has integer vertices. Let \( M(\triangle_0) = \{ \overline{f} | \triangle(\overline{f}) = \triangle_0 \} \). For each \( \overline{f} \in M(\triangle) \), \( \deg L(\overline{f}, T)^{(-1)^{n+1}} \leq n! \text{vol}(\triangle_0) \). Now we ask two questions: Does there exist \( \overline{f} \in M(\triangle) \) such that \( \deg L = n! \text{vol}(\triangle) \)? If so, if you grab \( \overline{f} \) at random in \( M(\triangle) \) does \( \deg L = n! \text{vol}(\triangle) \) still hold? It turns out that the answer to both of these questions is yes. The reason is that "smooth \( \overline{f} \)" will satisfy \( \deg L = n! \text{vol}(\triangle) \) and smooth \( \overline{f} \) are dense in \( M(\triangle) \). We use the word smooth in quotes because we are not actually going to give a rigorous characterization for smooth here.

Now we move on to the total degree estimate. Again, we know that
\[
L(\overline{f}, T) = \frac{\prod^{R}(1 - a_i T)}{\prod^{S}(1 - b_j T)}
\]
The total degree is \( R + S \).

Recall that
\[
L(\overline{f}, T)^{(-1)^{n+1}} = \frac{\prod^{R}(1 - w_i T)}{\prod^{S}(1 - \eta_j T)} = \det(1 - \alpha_a T)^{\delta_n}
\]
Write
\[
\det(1 - \alpha_a T)^{\delta_n} = \prod_{m=0}^{n} \det(1 - q^m \alpha_a T)^{(-1)^{m}(\frac{n}{m})}
\]
Hence, all zeros and poles of \( L(\overline{f}, T) \) occur as zeros of
\[
\prod_{m=0}^{n} \det(1 - q^m \alpha_a T)^{\left(\frac{n}{m}\right)} \tag{15}
\]
Fact (due to Deligne): \( 0 \leq \ord_q(w_i), \ord_q(\eta_j) \leq n \). Thus, all zeros and poles of \( L(\overline{f}, T) \) occur as zeros of equation (1) whose \( \ord_q \leq n \).

Let \( N_m := \text{number of zeros of } \det(1 - q^m \alpha_a T) \text{ of } \ord_q \leq n \). Thus, the total degree of \( L(\overline{f}, T) \) is \( \leq \sum_{m=0}^{n} N_m(n) \). Notice that \( N_m = \text{number of zeros of } \det(1 - \alpha_a T) \text{ with } \ord_q \leq n - m \).

Proposition.
\[
N_m \leq \sum_{j=1}^{r(m)} w(j)
\]
where \( r(m) \) is some number dependent on \( m \).

Thus the total degree is
\[
\leq \sum_{m=0}^{n} \left( \sum_{j=0}^{r(m)} w(j) \right) \left( \frac{n}{m} \right)
\]

Proposition. For all \( N \),
\[
\sum_{j=0}^{N} w(j) \leq \tilde{n}! \text{vol}(\triangle) \left( \frac{\frac{N}{\tilde{n}}}{\tilde{n}} \right) \left( \frac{n}{\tilde{n}} \right)
\]
Assuming this, the total degree is
\[
\leq \sum_{m=0}^{n} \tilde{n}! \text{vol}(\triangle) \left( \frac{\frac{N}{\tilde{n}}}{\tilde{n}} \right) \left( \frac{n}{\tilde{n}} \right)
\]
One can show that
\[
\left( \frac{N + \tilde{n}}{\tilde{n}} \right) \leq 2^{N + \tilde{n} - 1}
\]
for all \( N \), so the total degree is
\[
\leq \sum_{m=0}^{n} \tilde{n}! \text{vol}(\triangle)2^{\frac{r(m)}{N} + \tilde{n} - 1} \left( \frac{n}{m} \right)
\]

34
Now let

\[ r_0 = \max_{m=0}^r \left( \frac{r(m)}{D} \right) \]

This gives us that the total degree is

\[ \leq \tilde{n} \text{vol}(\Delta) 2^{r_0 + \tilde{n} - 1} \sum_{m=0}^n \binom{n}{m} \]

\[ = \tilde{n} \text{vol}(\Delta) 2^{\tilde{n} + n + 1} \]

17 Lecture 15 - Dillon

18 Lecture 16 - Brendan

18.1 Lower bounds for the degree of \( L(\tilde{f}, T)^{(−1)^n+1} \)

Previously we have shown that the \( L \)-function associated to \( \tilde{f} \) is rational:

\[ L(\tilde{f}, T)^{(−1)^n+1} = \prod_{i=1}^R \frac{(1 - \omega_i T)}{\prod_{j=1}^S (1 - \eta_j T)} \]

Further, we showed that the degree \( R - S \) is bounded by \( n! \text{vol}(\Delta) \) and that the total degree \( R + S \) is bounded above by a quantity involving \( \tilde{n} \) and \( \text{vol}(\Delta) \), where \( \Delta \) is the Newton polygon of \( \tilde{f} \) and \( \tilde{n} \) is the dimension of \( \Delta \). Today we will show that \( R - S \) is non-negative.

Let \( Z = \{\omega_1, \ldots, \omega_R\} \) be the multiset of zeros and let \( P = \{\eta_1, \ldots, \eta_S\} \) be the multiset of poles (so that repeated roots and poles are represented as distinct elements of \( Z \) and \( P \)). We say that \( \gamma_1, \gamma_2 \in Z \cup P \) are \( q \)-related if there is a \( t \) in \( Z \) such that \( \gamma_1 = q^t \gamma_2 \). It is easy to see that \( q \)-relatedness is an equivalence relation, so \( Z \cup P \) can be partitioned into equivalence classes of \( q \)-related elements. Let \( \mathcal{E} = \{E_1, \ldots, E_\ell\} \) be the set of equivalence classes. Note that no bounds on the number \( \ell \) of equivalence classes are known.

Fix \( E \in \mathcal{E} \) and define

\[ L_E(\tilde{f}, T)^{(−1)^n+1} = \prod_{\omega \in Z \cap E} (1 - \omega T) \prod_{\eta \in P \cap E} (1 - \eta T) \]

Then

\[ L(\tilde{f}, T)^{(−1)^n+1} = \prod_{E \in \mathcal{E}} L_E(\tilde{f}, T)^{(−1)^n+1} \]

Note that \( L_E \) has not be studied \( p \)-adically like \( L \) has been studied. By abuse of notation, write

\[ L_E(\tilde{f}, T)^{(−1)^n+1} = \prod_{i=1}^{R_E} (1 - \omega_i T) \prod_{j=1}^{S_E} (1 - \eta_j T) \]

(We have abused the terms \( \omega_i \) and \( \eta_j \), since they do not necessarily correspond to the previous \( \omega_i \) and \( \eta_j \) that occur in \( L(\tilde{f}, T) \).)

**Proposition 18.1.** For all \( E \) in \( \mathcal{E} \), \( R_E - S_E \geq 0 \).

It quickly follows from this proposition that \( R - S \geq 0 \), as \( R = \sum_{E \in \mathcal{E}} R_E \) and \( S = \sum_{E \in \mathcal{E}} S_E \).

**Proof.** For each \( \gamma \in Z \cup P \), define

\[ H_\gamma(T) = \prod_{m=0}^\infty (1 - q^m \gamma T)^{c(m)}, \]

where \( c(m) = \binom{m + n - 1}{n-1} \). We have shown that

\[ \det(1 - \alpha_i T) = \frac{D_1(T)}{D_2(T)} = \prod_{\omega \in Z} H_\omega(T) \prod_{\eta \in P} H_\eta(T) \]

Note that \( \gamma_1 \) and \( \gamma_2 \) are \( q \)-related if and only if \( H_{\gamma_1}(T) \) and \( H_{\gamma_2}(T) \) share a common factor.

Writing

\[ D_{1,E}(T) = \prod_{\omega \in Z \cap E} H_\omega(T) \quad \text{and} \quad D_{2,E}(T) = \prod_{\eta \in P \cap E} H_\eta(T), \]

35
we have
\[
\det(1 - \alpha_s T) = \prod_{E \in \mathcal{E}} \frac{D_{1,E}(T)}{D_{2,E}(T)}.
\]

Since \(\det(1 - \alpha_s T)\) is \(p\)-adic entire, we know that \(D_2\) divides \(D_1\). By \(q\)-relatedness, factors in \(D_{2,E}(T)\) can only cancel with factors in \(D_{1,E}(T)\), thus \(D_{2,E}(T)\) divides \(D_{1,E}(T)\) and we may conclude that each quotient
\[
\frac{D_{1,E}(T)}{D_{2,E}(T)}
\]
is entire.

Fix \(\eta_i\) in \(P \cap E\). By \(q\)-relatedness, for \(i = 1, \ldots, R_E\) there exists a \(t_i \in \mathbb{Z} \setminus \{0\}\) such that
\[
\eta_i = q^{t_i} \omega_i.
\]
(Note that \(t_i\) cannot equal zero, because the \(L\)-function is in lowest terms, which implies that \(\eta_i \neq \omega_i\).

Since
\[
H_{\omega_i} = \prod_{m=0}^{\infty} (1 - q^m \omega_i T)^{c(m)},
\]
for \(t_i > 0\) we have
\[
H_{\omega_i} = \prod_{0 \leq m < t_i} (1 - q^m \omega_i T)^{c(m)} \prod_{m=0}^{\infty} (1 - q^{m+t_i} \omega_i T)^{c(m+t_i)},
\]
and for \(t_i < 0\) we have
\[
H_{\omega_i} = \prod_{m=-t_i}^{\infty} (1 - q^{m+t_i} \omega_i T)^{c(m+t_i)}.
\]

In either case, for \(m \geq 0\) we have that \((1 - q^m \eta_i T) = (1 - q^{m+t_i} \omega_i T)\) divides \(H_{\omega_i}(T)\) exactly \(c(m + t_i)\) times. Thus for all \(m \geq 0\), the number of times \(\prod_{i=1}^{R_E} H_{\omega_i}(T)\) is divisible by \((1 - q^m \eta_i T)\) is
\[
\sum_{i=1}^{R_E} c(m + t_i) = \sum_{i=1}^{R_E} \frac{(m + t_i + n - 1) \cdots (m + t_i + 1)}{(n - 1)!} = \frac{R_E}{(n - 1)!} m^{n-1} + O(m^{n-2}). \tag{16}
\]

A similar analysis can be made for the denominator \(\prod_{\eta \in P \cap E} H_\eta(T)\). That is, for each \(j = 1, 2, \ldots, S_E\), there exists \(s_j \in \mathbb{Z}\) such that \(\eta_j = q^{s_j} \eta_j\), and for \(m \geq 0\), the number of times \(\prod_{\eta \in P \cap E} H_\eta(T)\) is divisible by \((1 - q^m \eta_j T)\) is
\[
\sum_{j=1}^{S_E} c(m + s_j) = \frac{S_E}{(n - 1)!} m^{n-1} + O(m^{n-2}). \tag{17}
\]

Since
\[
\frac{D_{1,E}(T)}{D_{2,E}(T)} = \frac{\prod_{\omega \in \mathcal{E} \cap T} \prod_{m=0}^{\infty} (1 - q^m \omega T)^{c(m)}}{\prod_{\eta \in P \cap T} \prod_{m=0}^{\infty} (1 - q^m \eta T)^{c(m)}}
\]
is entire, each factor \((1 - q^m \eta T)\) in the denominator cancels with a factor in the numerator. Thus for all \(m \geq 0\), the terms in equation 16 are larger than the terms in equation 17. This can only be true if \(R_E \geq S_E\).

Many of the quantities appearing in the above proof have not been studied in detail. We collect a few questions here.

**Open Question 1.** Can you find bounds for \(R_E - S_E\) and \(R_E + S_E\)? No bounds are currently known.

**Open Question 2.** Can you bound the number of \(q\)-related equivalence classes?

**Open Question 3.** What can we learn about \(L_E\) using the \(p\)-adic methods we applied to \(L\)?
18.2 Variations of $L$-functions

We will now study $L$-functions that depend on a parameter. The prototype for this is the Kloosterman family:

$$f(t, x) := x + \frac{t}{x} \in \mathbb{F}_p[t, x^\pm].$$

Fix $\tilde{t} \in \mathbb{F}_{q}^*$ and consider

$$\tilde{f}(\tilde{t}, x) \in \mathbb{F}_q[x^\pm]$$

and the related toric exponential sum

$$S_m(\tilde{t}) = \sum_{\bar{x} \in \mathbb{F}_{q^m}^*} \psi \circ \text{Tr}(\tilde{f}(\tilde{t}, \bar{x})).$$

This is called a Kloosterman sum.

By our previous theory, we know that for fixed $\tilde{t}$,

$$L(\tilde{t}, \tilde{f}, T) = L(\tilde{t}, \tilde{f}, T)(-1)^{i+1} = \prod (1 - \omega T) \prod (1 - \eta T) \in \mathbb{Q}(\zeta_p)(T).$$

In fact, later we will see that

$$L(\tilde{t}, \tilde{f}, T) = (1 - \omega_1 T)(1 - \omega_2 T).$$

(Further, Weil showed that $|\omega_1|_C = \sqrt{q}$ and $\omega_1 \omega_2 = q$.)

Here is the main question we will investigate:

**Question 18.2.** How does $L(\tilde{t}, \tilde{f}, T)$ vary as $\tilde{t}$ varies in $\mathbb{F}_q^*$?

In particular, we might investigate how the degree changes, how the total degree changes, or how the roots vary

We will focus on the following variation. We will show that the $L$-functions associated to Kloosterman sums have a unique unit root: $\text{ord}_q(\omega_1) = 0$; in fact, we will show this for a more general family of functions. For Kloosterman sums, $\omega_1 \omega_2 = q$, so $\text{ord}_q(\omega_1) = 0$ implies $\text{ord}_q(\omega_2) = 1$. For each $\tilde{t} \in \mathbb{F}_q^*$, let $\pi_0(\tilde{t})$ denote the unique unit root of $L(\tilde{t}, \tilde{f}, T)$, and let $\pi_1(\tilde{t})$ denote the root with $\text{ord}_q = 1$. Thus

$$L(\tilde{t}, \tilde{f}, T) = (1 - \pi_0(\tilde{t}) T)(1 - \pi_1(\tilde{t}) T).$$

Our goal is to study $\pi_0(\tilde{t})$.

19 Lecture 17 - Siegfred

In the last lecture, we introduced the Kloosterman family $\tilde{f}_t(x) = x + \frac{t}{x} \in \mathbb{F}_p[t, x^\pm]$ and the Kloosterman sum

$$S_m(\tilde{t}) = \sum_{\bar{x} \in \mathbb{F}_{q^m}^*} \Psi \circ \text{Tr} \left( \bar{x} + \frac{\tilde{t}}{\bar{x}} \right).$$

We claimed (but did not prove) that

$$L(\tilde{f}_t, T) = (1 - \pi_0(\bar{t}) T)(1 - \pi_1(\bar{t}) T),$$

with $\text{ord}_q(\pi_i(\bar{t})) = i$. In particular there exists a unique unit reciprocal root $\pi_0(\bar{t})$ for each $\bar{t}$. We want to study how $L$ varies as $\bar{t}$ varies. For instance, we may ask:

**Question:** How does $\pi_0(\bar{t})$ vary as $\bar{t}$ varies?

One approach to study this question is to use Dwork’s unit root L-function, defined as follows, for fixed positive integer $k$:

$$L_{\text{unit}}(k, T) = \prod_{\bar{t} \in \mathbb{F}_{q^m}^*/\mathbb{F}_q} \left( \frac{1}{1 - \pi_0(\bar{t}) T^{\deg(\bar{t})}} \right)^{\deg(\bar{t})},$$

---

19 “Vary” requires some interpretation because we have no topology on $\mathbb{F}_q$.

20 Here, $\bar{t} \in \mathbb{F}_{q^m}^*$, so $q = q(\bar{t})$ depends on $\bar{t}$, and we define (as in the definition of $L(\tilde{f}_t, T)$ in the 10Oct lecture) $\Psi$ and $\text{Tr}$ in the usual way by considering $\tilde{f}_t$ as a Laurent polynomial in the $x$-variable, i.e. $\tilde{f}_t \in \mathbb{F}_q[x^\pm]$. Thus $\text{Tr}$ is the trace map relative to the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ and $\Psi : \mathbb{F}_q \to \mathbb{Q}_0(\pi)$ is the additive character $\bar{b} \mapsto \theta(1)^k$, where $\theta(1)$ is a primitive $p$th root of unity and $\xi$ is the trace of $\bar{b}$ relative to the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$.

21 This definition of $L_{\text{unit}}$ is a formal definition, and (as far as we know) may not converge for nonzero $T$. However, we will see below that if we reinterpret the product by grouping together the factors that correspond to Galois conjugates, then it converges for $|T|_p < 1$. 

37
where \( q \) is a fixed power of \( p \) and\(^{22} \) \( \deg(T) = |F_q(T) : F_q| \). The following is a special case of Dwork’s conjecture:

**Conjecture:** \( L_\text{unit}(k, T) \) is \( p \)-adic meromorphic.

Dwork’s conjecture was proved by Daqing Wan in a series of papers. Our goal is to prove Dwork’s conjecture for toric families. The family of Kloosterman sums is one example of a toric family.

Let \( \sigma \) be a Galois conjugate of \( T \), i.e. there exists a \( \sigma \) in \( \text{Gal}(F_q^\times) \) such that \( \sigma(T) = \sigma \). Note that \( \sigma(E^\times) = E^\times \) for any finite extension \( E \) of \( F_q \), because finite fields are normal extensions\(^{23} \) and homomorphisms always map 0 to 0. Thus\(^{24} \)

\[
S_m(T) = \sum_{T \in F_q^\times} \Psi \circ \text{Tr} \left( \tau + \frac{T}{x} \right) \quad \text{ (definition of } S_m(T) \text{ )}
\]

\[
= \sum_{T \in F_q^\times} \Psi \circ \text{Tr}(\sigma(\tau + \frac{T}{x}))
\]

\[
= \sum_{T \in F_q^\times} \Psi \circ \text{Tr} \left( \sigma(\tau) + \frac{\sigma(T)}{\sigma(x)} \right)
\]

\[
= \sum_{T \in F_q^\times} \Psi \circ \text{Tr} \left( \tau + \frac{\sigma(T)}{x} \right) \quad \text{because } \sigma \text{ permutes } \tau \in F_q^\times_{\sigma}.
\]

\[
S_m(\tau) = S_m(T).
\]

hence \( L(T, T) = L(T, T) \). Thus \( \pi_0(T) = \pi_0(\tau) \). Hence, in the definition of \( L_\text{unit} \), we can collect together the terms that have \( \tau \) as Galois conjugates, as follows. Denote by \( |\mathbb{G}_m/F_q| \) the set of orbits of the set \( F_q^\times \) under the action of \( \text{Gal}(F_q^\times/F_q) \). If \( [T] \in |\mathbb{G}_m/F_q| \) denotes the orbit of \( T \), then \( [T] \) is a subset of \( F_q(T) \) with \( |F_q(T) : F_q| = \deg(T) \) elements\(^{25} \). Thus\(^{26} \)

\[
L_\text{unit}(k, T) = \prod_{[T] \in |\mathbb{G}_m/F_q|} \prod_{\tau \in [T]} \left( 1 - \pi_0(\tau)^{kT\deg([T])} \right)^{\frac{1}{\deg([T])}}
\]

\[
= \prod_{[T] \in |\mathbb{G}_m/F_q|} \frac{1}{1 - \pi_0(\tau)^{kT\deg([T])}}.
\]

The unit root \( L \)-function for toric families

Let \( A \) be a finite nonempty subset of \( \mathbb{Z}^n \). Consider

\[
f(t, x) = \sum_{u \in A} t^u x^u \in F_p \{ t_u : u \in A \}, x_1^\pm, \ldots, x_n^\pm \]

Note that the coefficients of \( f(t, x) \) as an element of \( F_p \{ t_u : u \in A \}, x_1^\pm, \ldots, x_n^\pm \) are all 1. As with the Kloosterman

\(^{22}\) The “/\( F_q^\times \)” in the subscript \( \tau \in F_q^\times / F_q \) of the product symbol means that \( \deg(T) \) is the degree relative to \( F_q \), that is, \( \deg(T) = |F_q(T) : F_q| \). We still take the product over all \( \tau \) in \( F_q^\times \).

\(^{23}\) Recall that \( F_q^\times \) is the splitting field of the polynomial \( x^{p^n} - x \) over \( F_q \); thus it is normal because splitting fields are normal extensions. Hence, in any algebraic closure \( C \) of \( F_q^\times \), any monomorphism of \( F_q^\times \) into \( C \) is an automorphism of \( F_q^\times \).

\(^{24}\) Here, \( T \in F_q^\times \), and the functions \( \Psi \) and \( \text{Tr} \) are defined with respect to \( q_1 \), i.e. \( \text{Tr} \) is the trace map relative to the extension \( F_q^\times / F_{q_1} \) and \( \Psi : F_{q_1} \to F_{q_1} \) is the additive character \( b \to \theta(1)^b \), where \( p \) is the trace of \( b \) relative to the extension \( F_{q_1} / F_p \). Recall that \( \text{Trace}^F_{F_p}(a) = \text{Trace}^F_{F_p}(b) \) if \( a \) and \( b \) are Galois conjugates in \( E \) over \( F \) since \( \text{Trace}^F_{F_p}(a) \) is equal to the sum of the Galois conjugates of \( a \) over the base field \( F \). In the sum expression for \( S_m(T) \), it may be that \( \text{Tr}(\sigma(x + T/x)) \) is not equal to \( \text{Tr}(x + T/x) \) because \( \sigma(x + T/x) \) and \( x + T/x \) may not be Galois conjugates over \( F_{q_1} \). As with the Kloosterman

\(^{25}\) Recall that \( T \) has exactly \( \deg(T) \) Galois conjugates over \( F_q \) since finite extensions of \( F_p \) are separable. Separability comes from the fact that every element is a \( p \)-th power (the Frobenius automorphism). All Galois conjugates of \( T \) are in \( F_q(T) \) because \( F_q(T) \) is a normal extension of \( F_p \).

\(^{26}\) The resulting product expression for \( L_\text{unit} \) is convergent for \( |T|_p < 1 \). Indeed, since \( \pi_0(T) \) has ord\( _p \) equal to 0, each factor in the product can be written as \( 1 + \sum_{j=1}^\infty \pi_0(T)^{j k T \deg(T)} \) for such \( T \). The sum of the terms with \( j \geq 1 \) has norm at most \( |T|_p^{\deg(T)} \) by the ultrametric inequality. Thus the product converges because \( |T|_p^d \to 0 \) as \( d \to \infty \) when \( |T|_p < 1 \), and because there are only finitely many \( \tau \) with \( \deg(T) \leq A \), for each fixed positive integer \( A \). In \( C_p \), a product \( \prod_{\tau \in [T]} \) converges if and only if \( |a_n|_p \) tends to 0.
example, fix $\tilde{t} \in (\mathbb{F}_q^\times)^{|A|}$ and set $q_{\tilde{t}} := q^{|\deg(\tilde{t})|}$ and\footnote{Here, as in the definition of $L(f_{\tilde{t}}, T)$ in the 10Oct lecture, $\Psi : F_{q_{\tilde{t}}} \to Q_{q_{\tilde{t}}}(\pi)$ is the additive character $\tilde{t} \mapsto \theta(1)\xi$, where $\xi$ is the trace of $\tilde{t}$ relative to the extension $F_{q_{\tilde{t}}}/F_p$. The subscript $\tilde{t}$ serves as a reminder that the definitions depend on the fixed parameter $\tilde{t}$, which is an $|A|$-tuple. The degree $\deg(\tilde{t})$ still denotes $[F_{q_{\tilde{t}}}(\tilde{t}) : F_p]$, but we keep in mind that $\tilde{t}$ is an $|A|$-tuple, so that $F_{q_{\tilde{t}}}(\tilde{t})$ means precisely $F_q(t_u : u \in A)$. In any algebraic closure of $F_p$, there is exactly one finite field with $q_{\tilde{t}}$ elements, so we write $F_{q_{\tilde{t}}} := F_\ell(\tilde{t})$. Note also that, for such fixed $\tilde{t}$, $f_{\tilde{t}}$ has coefficients in $F_p$, when considered as a Laurent polynomial in the $x$-variables.}

\[
S_m(\tilde{t}) := \sum_{\pi_1, \ldots, \pi_n \in F_{q_{\tilde{t}}}} \Psi \circ \text{Tr}_{F_{q_{\tilde{t}}} / F_p}(f(\tilde{t}, \pi)).
\]

We will write $f_{\tilde{t}}(x) := f(\tilde{t}, x)$. We know\footnote{Rationality of the L-function was proved in the 17Oct lecture.}

\[
L(f_{\tilde{t}}, T)(-1)^{n+1} = \prod_{j=1}^{R} \frac{1 - \omega_i T}{1 - \eta_j T},
\]

where the degrees $R$, $S$, and the reciprocal roots $\omega_i$ and reciprocal poles $\eta_j$ may depend on $\tilde{t}$. Thus they may change when $\tilde{t}$ changes. However, we have the following.

**Proposition.** $L(f_{\tilde{t}}, T)(-1)^{n+1}$ has a unique unit reciprocal root for each $\tilde{t} \in (\mathbb{F}_q^\times)^{|A|}$.

**Proof.** From our construction of the additive character $\Psi$, we have $\Psi(b) := \theta(1)\text{Tr}_{F_p / F_q}(b)$, where $\theta(1)$ is a primitive $p$th root of unity. We showed $\text{ord}_p(\theta(1) - 1) = \frac{1}{p-1}$. Set $\gamma := \theta(1) - 1$, so $\theta(1) = 1 + \gamma$. The idea is to see what happens when we reduce mod $\gamma$. We have

\[
S_m(\tilde{t}) = \sum_{\pi} \Psi \circ \text{Tr}_{F_{q_{\tilde{t}}} / F_p}(f_{\tilde{t}}(\pi)) \quad \text{(definition of } S_m(\tilde{t}))
\]

\[
= \sum_{\pi} \theta(1) \text{Tr}_{F_{q_{\tilde{t}}} / F_p}(f_{\tilde{t}}(\pi))
\]

\[
= \sum_{\pi} (1 + \gamma)\text{Tr}(f_{\tilde{t}}(\pi))
\]

\[
= \sum_{\pi} 1 \pmod{\gamma} \quad \text{by binomial expansion of } (1 + \gamma)\text{Tr}(f_{\tilde{t}}(\pi))
\]

\[
= (q_{\tilde{t}}^m - 1)^n \pmod{\gamma}
\]

because $q_{\tilde{t}}$ is a power of $p$ and because $p = \gamma(\gamma^{-1}p)$ with $\text{ord}_p(\gamma^{-1}p) = -\frac{1}{p-1} + 1 \geq 0$. Now

\[
L(f_{\tilde{t}}, T)(-1)^{n+1} = \exp \left( -1)^{n+1} \sum_{m=1}^{\infty} S_m(\tilde{t}) \frac{T_m}{m} \right) \quad \text{(definition of } L)
\]

\[
= \exp \left( -1)^{n+1} \sum_{m=1}^{\infty} (1 - \gamma^n) \frac{T_m}{m} \right) \pmod{\gamma}
\]

\[
= \exp \left( - \sum_{m=1}^{\infty} \frac{T_m}{m} \right)
\]

\[
= 1 - T
\]

In particular, $L(f_{\tilde{t}}, T)(-1)^{n+1} \equiv 0 \pmod{\gamma}$. Thus $1 - \omega_i \equiv 0 \pmod{\gamma}$ for some $i$, so $\omega_i \in 1 + \gamma\mathbb{Z}_p$ and $\text{ord}_p(\omega_i) = 0$ for some $i$. This shows that $L(f_{\tilde{t}}, T)(-1)^{n+1}$ has at least one unit reciprocal root, i.e. this shows existence of a unit reciprocal root.

It may be possible some factors of the denominator of $L(f_{\tilde{t}}, T)(-1)^{n+1}$ cancel with the factors of the numerator with unit reciprocal roots when we reduce mod $\gamma$. To show uniqueness of the unit reciprocal root, we will show that this does not happen. The Dwork Trace formula gives

\[
L(f_{\tilde{t}}, T)(-1)^{n+1} = \det(1 - \alpha_a T)^{\delta_n},
\]

where $\delta$ is the operator that sends the function $g(T)$ to the function $g(T)/g(q_{\tilde{t}}T)$, so

\[
L(f_{\tilde{t}}, T)(-1)^{n+1} = \det(1 - \alpha_a T) \cdot \prod_{m=1}^{n} \det(1 - q_{\tilde{t}}^m\alpha_a T)^{(-1)^m(n)}.
\]
Each factor in the product on the right above with \( m \geq 1 \) has all reciprocal zeros divisible by \( q_p \) and thus equal to 0 mod \( \gamma \). Hence
\[
\prod_{m=1}^{n} \det(1 - q_p^m \alpha T)^{-1/m} \equiv 1 \mod \gamma,
\]
so no unit reciprocal root or unit reciprocal pole of \( L(f,T)^{(-1)^{n+1}} \) is in the above product; hence all the unit reciprocal roots and unit reciprocal poles are in \( \det(1 - \alpha T) \). But \( \det(1 - \alpha T) \) is entire; hence \( L(f,T)^{(-1)^{n+1}} \) has no unit reciprocal poles, i.e. the denominator of \( L(f,T)^{(-1)^{n+1}} \) has no unit reciprocal roots. Now there cannot be more than 1 unit reciprocal root because we got \( 1 - T \mod \gamma \) and not \( (1 - T)^m \) for some \( m > 1 \) when reducing \( L(f,T)^{(-1)^{n+1}} \mod \gamma \). Thus there can only be at most one unit reciprocal root. This shows uniqueness of the unit reciprocal root. □

This proof has a problem. An alternative proof is: \( S_1(\ell) \) is congruent to \( (-1)^n \) modulo \( \pi \). We also know \( S_1 \) is a sum of the reciprocal zeros and poles of the \( L \)-function. Since the reciprocal zeros and poles have \( \text{ord}_p \geq 0 \), the only way for the sum to have \( \text{ord}_p(S_1) = 0 \) is that at least one of the zeros or poles also satisfies \( \text{ord}_p = 0 \).

20 Lecture 18 - Jamie

Last time we showed \( L(f,T)^{(-1)^{n+1}} \) has a unique unit root \( \pi_0(\bar{\ell}) \). Further, it has the property that \( \pi_0(\bar{\ell}) \equiv \mod (\pi) \) where \( \pi \) was a root of \( \sum_{i=0}^{\infty} \frac{a^i}{p^i} \) with \( \text{ord}_p(\pi) = \frac{1}{p-1} \).

To see this last part, we showed \( L(f,T)^{(-1)^{n+1}} \equiv 1 - T \mod (\pi) \implies \pi_0(\bar{\ell}) \equiv \mod (\pi).

For \( k \in \mathbb{Z}_{\geq 1} \), unit root \( L \)-function:
\[
L_{\text{unit}}(k,T) := \prod_{\bar{\ell} \in \mathbb{Q}[1/p]} \frac{1}{1 - \pi_0(\bar{\ell})T^{\deg(\bar{\ell})}}\]

Since there are only finitely many \( \bar{\ell} \) with bounded \( \deg(\bar{\ell}) \), \( L_{\text{unit}}(k,T) \in 1 + T\mathbb{Q}_{\bar{\ell}}[[T]] \). So, the Newton polygon of \( L_{\text{unit}}(k,T) \) lies on or above the -axis. Thus, \( L_{\text{unit}} \) converges of \( |T| < p^0 = 1 \).

Goal: Show \( L_{\text{unit}} \) analytically (meromorphically) continues to \( \mathbb{C}_p \).

Note, if \( a \) is a unit, then \( a^k \) makes sense for \( k \in \mathbb{Z}_p \). So it makes sense to define \( L_{\text{unit}}(k,T) \) with \( k \in \mathbb{Z}_p \). View \( L_{\text{unit}}(k,T) \) as a two variable function on \( \mathbb{Z}_p \times \mathbb{C}_p \). (The set \( L_{\text{unit}} = 0 \) in \( \mathbb{Z}_p \times \mathbb{C}_p \) is related to the Eigencurve.)

For each \( \bar{\ell} \): \( L(f,T) = (1 - \pi_0(\bar{\ell})T)\ldots(1 - \pi_N(\bar{\ell})T) \in \mathbb{Q}(\zeta_p)[T] \)

Remark.
\[
M(k,T) = \prod_{\bar{\ell} \in \mathbb{Q}[1/p]} \frac{1}{(1 - \pi_0(\bar{\ell})T^{\deg(\bar{\ell})})\ldots(1 - \pi_N(\bar{\ell})T^{\deg(\bar{\ell})})}
\]

since \( \pi_0(\bar{\ell}) \) is a 1-unit: \( \lim_{m \to \infty} \pi_0(\bar{\ell})^{k+p^m} = \pi_0(\bar{\ell}) \) and \( \lim_{m \to \infty} \pi_i(\bar{\ell})^{k+p^m} = 0 \) for \( i \neq 0 \). So \( \lim_{m \to \infty} M(k + p^m,T) = L_{\text{unit}}(k,T) \).

21 Some Linear Algebra

Let \( V \) be a finite dimensional vector space with basis \( e_1, \ldots, e_r \) over a field of characteristic 0.

- \( \text{Sym}^k(V) \) = span of vectors \( e_{i_1} \ldots e_{i_r} \) such that \( i_1 + \ldots + i_r = k \), \( i_1, \ldots, i_r \in \mathbb{Z}_{\geq 0} \)

- \( \Lambda^k(V) \) = span of vectors \( e_{i_1} \wedge \ldots \wedge e_{i_k} \) with \( 1 \leq i_1 < \ldots < i_k \leq r \) (kth exterior power).

Note, \( \Lambda^k(V) = 0 \) if \( k > r \).

If \( E : V \to V \) is a linear transformation, define \( \text{Sym}^k(E) : \text{Sym}^k(V) \to \text{Sym}^k(V) \) and \( \Lambda^k(E) : \Lambda^k(V) \to \Lambda^k(V) \) by \( \text{Sym}^k(E)(e_{i_1} \ldots e_{i_r}) := (Ee_1)^{i_1} \ldots (Ee_r)^{i_r} \) and \( \Lambda^k(E)(e_{i_1} \wedge \ldots \wedge e_{i_k}) := (Ee_{i_1}) \wedge \ldots \wedge (Ee_{i_k}) \).
Example:

\[ \dim(V) = 2 \]
\[ E(e_1) = ae_1 + be_2 \]
\[ E(e_2) = ce_1 + de_2 \]

\[ \text{Sym}^2(E)(e_1^2) = (Ee_1)^2 \]
\[ = (ae_1 + be_2)^2 \]
\[ = a^2e_1^2 + 2abe_1e_2 + b^2e_2^2 \]

\[ \bigwedge^2(E)(e_1 \wedge e_2) = (Ee_1) \wedge (Ee_2) \]
\[ = (ae_1 + be_2) \wedge (ce_1 + de_2) \]
\[ = ace_1 \wedge e_1 + bce_2 \wedge e_1 + ade_1 \wedge e_2 + bde_2 \wedge e_2 \]
\[ = (ad - bc)e_1 \wedge e_2 \]

**Proposition 21.1.**

\[ \det(1 - ET) = \sum_{i \geq 0} (-1)^i \text{Tr}(\bigwedge^i E)^i \]
\[ \frac{1}{\det(1 - ET)} = \sum_{j \geq 0} \text{Tr}(\text{Sym}^j E)^j \]
\[ \frac{1}{\det(1 - ET)} = \exp \left( \sum_{k=1}^{\infty} \frac{\text{Tr}(E^k)}{k} T^k \right) \]

**Proof.** Idea: Assume

\[ E = \begin{pmatrix} \lambda_1 \\ & \ddots \\ & & \lambda_r \end{pmatrix} \]

Easy to show

\[ \bigwedge^i(E) = \begin{pmatrix} \cdots \\ \lambda_{i_1} \cdots \lambda_{i_k} \\ \cdots \end{pmatrix} \quad 1 \leq i_1 < \ldots < i_k \leq r \]

and

\[ \text{Sym}^k(E) = \begin{pmatrix} \cdots \\ \lambda_1^{i_1} \cdots \lambda_r^{i_r} \\ \cdots \end{pmatrix} \quad i_1 + \ldots + i_r = k \]

Compute

\[ \sum_{k=0}^{\infty} (-1)^k \text{Tr}(\bigwedge^k E)T^k = \sum_{k=0}^{\infty} (-1)^k \left( \sum_{1 \leq i_1 < \ldots < i_k \leq r} \lambda_{i_1} \ldots \lambda_{i_k} \right) T^k \]

Compute

\[ \det(1 - ET) = \prod_{i=1}^{r} (1 - \lambda_i T) = \sum_{k=0}^{\infty} (-1)^k \left( \sum_{1 \leq i_1 < \ldots < i_k \leq r} \lambda_{i_1} \ldots \lambda_{i_k} \right) T^k \]

Similar computation shows

\[ \frac{1}{\det(1 - ET)} = \prod_{i=1}^{r} \frac{1}{1 - \lambda_i T} = \prod_{i=1}^{r} \left( \sum_{l=0}^{\infty} (\lambda_i T)^l \right) \]
\[ = \sum_{k=0}^{\infty} \left( \sum_{i_1 + \ldots + i_k = 0} \lambda_1^{i_1} \ldots \lambda_r^{i_r} \right) T^k \]
\[ = \sum_{k=0}^{\infty} \text{Tr}(\text{Sym}^k E)T^k \]
In our remarks we looked at
\[
(1 - \pi_0(t)^k T^{\deg(t)}) \ldots (1 - \pi_N(t)^k T^{\deg(t)})
\]
set
\[
E = \begin{pmatrix}
\pi_0(t) \\
\vdots \\
\pi_N(t)
\end{pmatrix}
\]
then
\[
(1 - \pi_0(t)^k T^{\deg(t)}) \ldots (1 - \pi_N(t)^k T^{\deg(t)}) = \frac{1}{\det(1 - E^k T)}
\]
we want to rewrite this.

**Lemma 21.2.**

\[
\text{Tr}(E^k) = \sum_{i=1}^{k} (-1)^{i-1} \text{Tr}(\text{Sym}^{k-i} E) \text{Tr}(\bigwedge^i E)
\]

**Proof.** We know \( \frac{1}{\det(1 - ET)} = \exp \left( \sum_{k=1}^{\infty} \frac{\text{Tr}(E^k)}{k} T^k \right) \) take \( \frac{d}{dT} \log \) of both sides.

\[
- \frac{T \frac{d}{dT} \det(1 - ET)}{\det(1 - ET)} = \sum_{k=1}^{\infty} \text{Tr}(E^k) T^k
\]

Now,
\[
\det(1 - ET) = \sum_{i=0}^{\infty} (-1)^i \text{Tr}(\bigwedge^i E) T^i
\]
and
\[
\frac{1}{\det(1 - ET)} = \sum_{j=0}^{\infty} \text{Tr}(\text{Sym}^j E) T^j
\]

\[
- \frac{T \frac{d}{dT} \det(1 - ET)}{\det(1 - ET)} = \sum_{i=0}^{\infty} (-1)^i \text{Tr}(\bigwedge^i E) T^i \left( \sum_{j=0}^{\infty} \text{Tr}(\text{Sym}^j E) T^j \right)
\]

Look at the coefficient of \( T^k \):

\[
\sum_{i+j=k} (-1)^{i-1} \text{Tr}(\bigwedge^i E) \text{Tr}(\text{Sym}^j E) = \sum_{i=1}^{k} (-1)^{i-1} \text{Tr}(\bigwedge^i E) \text{Tr}(\text{Sym}^{k-i} E)
\]

22 Lecture 19 - Malcolm

The following is useful, but not necessary:

**Lemma 22.1.**

\[
\text{Tr}(E^k) = \text{Tr}(\text{Sym}^k E) + \sum_{i \geq 2} (-1)^{i-1} \cdot (i - 1) \cdot \text{Tr}(\text{Sym}^{k-i} E) \cdot \text{Tr}(\bigwedge^i E)
\]

**Proof.** We start with

\[
1 = \frac{\det(1 - ET)}{\det(1 - ET)} = \left( \sum_{i \geq 0} (-1)^i \cdot \text{Tr}(\bigwedge^i E) \cdot T^i \right) \left( \sum_{j \geq 0} \text{Tr}(\text{Sym}^j E) \cdot T^j \right).
\]

Since this power series in \( T \) is 1, the coefficient of \( T^k \) for \( k \geq 1 \) must be zero. So, the coefficient of \( T^k \) is:

\[
\sum_{i \geq 0} (-1)^i \cdot \text{Tr}(\text{Sym}^{k-i} E) \cdot \text{Tr}(\bigwedge^i E) = 0
\]

The result follows from the previous lemma.
Lemma 22.2. If $E_1$ and $E_2$ are matrices, then $\text{Tr}(E_1) \text{Tr}(E_2) = \text{Tr}(E_1 \otimes E_2)$.

Proof. Let $v_1, \ldots, v_n$ be a basis for $V$ and assume $E_1$ and $E_2$ are diagonalized

\[
E_1 = \begin{pmatrix}
\lambda_1 & & \\
& \ddots & \\
& & \lambda_n
\end{pmatrix}, \quad E_2 = \begin{pmatrix}
\lambda'_1 & & \\
& \ddots & \\
& & \lambda'_n
\end{pmatrix}.
\]

Then a basis for $V \otimes V$ is $\{v_i \otimes v_j \mid 1 \leq i, j \leq n\}$. The matrix $E_1 \otimes E_2$ then acts on the basis elements as follows:

\[(E_1 \otimes E_2)(v_i \otimes v_j) = (E_1v_i) \otimes (E_2v_j) = (\lambda_i v_i) \otimes (\lambda'_j v_j) = \lambda_i \lambda'_j (v_i \otimes v_j).
\]

Thus $\lambda_i \lambda'_j$ is an eigenvalue of $E_1 \otimes E_2$ and thus

\[
E_1 \otimes E_2 = \begin{pmatrix}
\ddots & \lambda_i \lambda'_j & \\
& \ddots & \\
& & \ddots
\end{pmatrix}_{1 \leq i, j \leq n}
\]

Therefore

\[
\text{Tr}(E_1 \otimes E_2) = \sum_{i,j=1}^{n} \lambda_i \lambda'_j = \left( \sum_{i=1}^{n} \lambda_i \right) \left( \sum_{j=1}^{n} \lambda'_j \right) = \text{Tr}(E_1) \text{Tr}(E_2).
\]

(Note we could have used two vector spaces $V$ and $W$)

We can now replace $\text{Tr}(\text{Sym}^{k-i}E) \cdot \text{Tr}(\wedge^i E)$ by $\text{Tr}(\text{Sym}^{k-i}E \otimes \wedge^i E)$. We now reach our goal lemma.

Lemma 22.3.

\[
\det(1 - E^k T) = \prod_{i \geq 1} \det\left(1 - (\text{Sym}^{k-i}E \otimes \wedge^i E) T\right)^{(-1)^{i-1} - i}.
\]

Proof. Write

\[
\det(1 - E^k T) = \exp \left(- \sum_{m=1}^{\infty} \text{Tr}(E^{km}) \frac{T^m}{m}\right)
\]

\[
= \exp \left(- \sum_{m=1}^{\infty} \left( \sum_{i \geq 1} (-1)^{i-1} \cdot i \cdot \text{Tr} \left( \text{Sym}^{k-i}E^m \otimes \wedge^i E^m \right) \right) \frac{T^m}{m}\right)
\]

\[
= \exp \left(- \sum_{m=1}^{\infty} \left( \sum_{i \geq 1} (-1)^{i-1} \cdot i \cdot \text{Tr} \left( \text{Sym}^{k-i}E \otimes \wedge^i E^m \right) \right) \frac{T^m}{m}\right)
\]

\[
= \prod_{i \geq 1} \exp \left(- \sum_{m=1}^{\infty} (-1)^{i-1} \cdot i \cdot \text{Tr} \left( \text{Sym}^{k-i}E \otimes \wedge^i E^m \right) \frac{T^m}{m}\right)
\]

\[
= \prod_{i \geq 1} \det \left(1 - (\text{Sym}^{k-i}E \otimes \wedge^i E) T\right)^{(-1)^{i-1} - i}.
\]

Let $A \subseteq \mathbb{Z}^n$ and $\tilde{t} \in \left(\mathbb{F}_q^*\right)^{|A|}$, $\tilde{t} = (\tilde{t}_1, \ldots, \tilde{t}_{|A|})$. We define

\[
\deg(\tilde{t}) := |\mathbb{F}_q(\tilde{t}_1, \ldots, \tilde{t}_{|A|}) : \mathbb{F}_q| = q^{\deg(t)}
\]

and set $q_{\tilde{t}} := q^{\deg(\tilde{t})}$. Let $\tilde{t} = \text{Teich}(\tilde{t}) = (\tilde{t}_1, \ldots, \tilde{t}_{|A|})$ and consider $f(t, x) = \sum_{u \in A} t_u x^u$ and its specialization $f_t(x) = f(\tilde{t}, x) \in \mathbb{F}_{q_{\tilde{t}}}[x_1^\pm, \ldots, x_n^\pm]$. For the sequence of exponential sums

\[
S_m(\tilde{t}) = \sum_{\tilde{x}_1, \ldots, \tilde{x}_n \in \mathbb{F}_{q_{\tilde{t}}}^n} \psi \circ \text{Tr}(f_t(\tilde{x}))
\]

43
the associated \(L\)-function \(L(f_t, T) \in \mathbb{Q}(\zeta_p)(T)\) is rational with bounds on the degree and total degree. From that theory (recall the definition of \(\alpha_a\)) with \(\alpha_{ad(t)}\) where \(d(t) = \deg(t)\) defined to be

\[
\alpha_{ad(t)} := \psi q_t \circ \Gamma_{ad(t)}(t, x)
\]

being an endomorphism of

\[
C_{0,t} = \left\{ \sum_{u \in M} c_u \pi^{w(u)} u \mid \hat{\pi} = \pi^{1/D}, c_u \in \mathbb{Z}_q, c_u \to 0 \text{ as } w(u) \to \infty \right\}.
\]

We have \(L(f_t, T)^{(-1)^{n+1}} = \det(1 - \alpha_{ad(t)}T)\delta^p\) where

\[
\delta_t : g(T) \mapsto \frac{g(T)}{\gamma(q_1T)}.
\]

We have shown that for each \(\bar{t} \in \mathbb{G}_m\), \(L(f_t, T)^{(-1)^{n+1}}\) has a unique unit root \(\pi_0(\bar{t})\). Further, because of the \(\delta_t\) operator, \(\pi_0(\bar{t})\) must be a reciprocal eigenvalue of \(\det(1 - \alpha_{ad(t)}T)\). All other reciprocal roots of this must have \(\text{ord}_T > 0\). Note: We use \(\text{ord}_T\) here since we showed \(L(f_t, T)^{(-1)^{n+1}} \equiv 1 - T \pmod{(\pi)}\). Thus, for \(k \geq 1\), \(\pi_0(\bar{t})^k\) is the unique unit root of \(\det(1 - \alpha_{ad(t)}^kT)\) and all other reciprocal roots have \(\text{ord}_T > 0\). That is to say

\[
\det(1 - \alpha_{ad(t)}^kT) = \prod_{i=0}^{\infty} \left(1 - \pi_i(\bar{t})^kT\right)
\]

where \(\pi_i(\bar{t})\) are the reciprocal roots, \(\text{ord}_T(\pi_0(\bar{t})) = 0\), and \(\text{ord}_T(\pi_i(\bar{t})) > 0\) for \(i \geq 1\). Since \(\lim_{m \to \infty} k + p^m = k\) \(p\)-adically, we have that

\[
\lim_{m \to \infty} \det \left(1 - \alpha_{ad(t)}^{k+p^m}T\right) = \det(1 - \pi_0(\bar{t})^kT).
\]

Thus we some linear algebra we have that

\[
L_{\text{unit}}(k, T) = \lim_{m \to \infty} \prod_{i \geq 0} W_{(k+p^m, i)}(T)^{(-1)^i - i}
\]

where

\[
W_{(k,i)} := \prod_{\bar{t} \in \mathbb{G}_m^{[E:F_q]}} \frac{1}{\det \left(1 - (\text{Sym}^{k-i} \alpha_{ad(t)} \otimes \Lambda^i \alpha_{ad(t)})T^d(t)\right)}
\]

23 Lecture 20 - Meg

We would like to show that \(\pi_0(\bar{t})^{k+p^m} \to \pi_0(\bar{t})^k\) as \(m \to \infty\).

To do this, assume that \(\alpha = 1 + \pi \beta\) with \(\text{ord}_p(\pi) > 0\) and \(\text{ord}_p(\beta) \geq 0\) and \(\pi\) the uniformizer.

As a side note, recall our setup from much earlier:

\(\alpha \in E, [E:Q_p] < \infty\)

\(O = \{x \in E ||x| \leq 1\}\)

\(\mathcal{M} = \{x \in E ||x| < 1\}\)

\(\pi = \text{Teichm"uller}\)

\(1 = \pi = \text{Im}(\alpha)\) in \(O/\mathcal{M} = \mathbb{F}_q\). Call \(\alpha\) a 1-unit (principal unit). In a previous lecture, we showed that \(\pi_0(\bar{t})\) is a 1-unit for all \(\bar{t}\).

**Lemma 23.1.**

\[
\lim_{m \to \infty} \alpha^{p^m} = 1
\]

(In general, for \(\alpha \in O\), \(\lim_{m \to \infty} \alpha^{p^m} = \alpha_0\), where \(\alpha_0\) is the Teichmüller of \(\alpha\), meaning that \(\alpha_0\) is the Teichmüller of \(\pi = \text{Im}(\alpha)\) in \(O/\mathcal{M}\).)
Proof. We will show that $|\alpha^p - 1| \leq |\pi|^{m+1}$ for all $m$. Then, since $|\pi|^{m+1} \to 0$ as $m \to \infty$, we will have our result.

To show this, we will use induction. First, consider $m = 0$. Then $|\alpha - 1| = |\pi| \leq |\pi|$.

Now assume that the statement is true for $m$, so $|\alpha^p - 1| \leq |\pi|^{m+1}$. This implies that $\alpha^p - 1 = \pi^{m+1}\beta'$ for some $\beta'$ with $\text{ord}_p(\beta') \geq 0$, since $\pi$ is a uniformizer. Then,

$$(\alpha^p)^p = (1 + \pi^{m+1}\beta')^p$$

so

$$\alpha^{p+1} = 1 + \sum_{i=1}^p \binom{p}{i}(\pi^{m+1}\beta')^i$$

Notice that for $1 \leq i \leq p - 1$,

$$\binom{p}{i}(\pi^{m+1}\beta')^i$$

is divisible by $p\pi^{m+1}$, and for $i = p$,

$$\binom{p}{p}(\pi^{m+1}\beta')^i$$

is divisible by $\pi^{(m+1)p}$. This implies that $|\alpha^{p+1} - 1| \leq |\pi|^{m+2}$. \hfill $\square$

Recall from last time that $L_{\text{unit}}(k, T) = \lim_{m \to \infty} \prod_{i \geq 1} w_{k+p^m,i}(T)^{-1-i}$

where

$$w_{k,i}(T) := \prod_{\gamma \in \text{Ad}_{\alpha(k,i)} \otimes \mathbb{Q}} \frac{1}{\det(1 - \alpha(k,i) T^{d\text{deg}(\gamma)})}$$

where $\alpha^{(k,i)}_{\text{ad}(\gamma)} := \text{Sym}^k \alpha_{\text{ad}(\gamma)} \otimes \bigwedge^i \alpha_{\text{ad}(\gamma)}$

Goal: Show that $\lim_{m \to \infty} w_{k+p^m,i}(T)$ is $p$-adic meromorphic.

To motivate this, notice that in above limit, $i$ is fixed, and

$$\text{Sym}^{k+p^m-i} \to \text{Sym}^\infty$$

where $\text{Sym}^\infty$ is an infinite symmetric power. Right now, $\alpha_{\text{ad}(\gamma)} : C_{0,\overline{T}} \to C_{0,\overline{T}}$ where $C_{0,\overline{T}}$ has basis $\{\pi^{u_1} x^{u}\}_{u \in \Delta}$. Then $\text{Sym}^k \alpha_{\text{ad}(\gamma)} : \text{Sym}^k C_{0,\overline{T}} \to \text{Sym}^k C_{0,\overline{T}}$.

A basis for $\text{Sym}^k C_{0,\overline{T}}$ is as follows:

Order the basis of $C_{0,\overline{T}}$ as

$$(1, \pi^{w(1)} x^{u_1}, \ldots) = (e_{u_0}, e_{u_1}, \ldots)$$

and such that $w(u_i) \to \infty$ as $i \to \infty$. (If we define $|e^u| := |\pi|^{w(u)}$, then insist that $|e_{u_{i+1}}| \leq |e_{u_i}|$.)

Then a basis for $\text{Sym}^k C_{0,\overline{T}}$ is

$$\{e_{u_1} \cdots e_{u_k} | i_1, \ldots, i_k \in \mathbb{Z}_{\geq 1}\}$$

$$= \{e^{k-r}_{u_0} e_{u_1} \cdots e_{u_r} | i_1, \ldots, i_r \in \mathbb{Z}_{\geq 1}\} \bigcup \{e_{u_1} \cdots e_{u_k} | i_1, \ldots, i_k \in \mathbb{Z}_{\geq 1}\}$$

We think that $\text{ord}_p(e_{u_1} \cdots e_{u_k}) = w(u_{i_1}) + \cdots + w(u_{i_k})$. Now think of replacing $k$ by $k + p^m$ and letting $m \to \infty$. Then all terms in $\{e_{u_1} \cdots e_{u_k} | i_1, \ldots, i_k \in \mathbb{Z}_{\geq 1}\}$ have $\text{ord}_p \to \infty$. This leaves $\{e^{k-r}_{u_0} e_{u_1} \cdots e_{u_r} | i_1, \ldots, i_r \in \mathbb{Z}_{\geq 1}\}$ for $r$ fixed.

$$e^{k+r-p}_{u_0} e_{u_1} \cdots e_{u_r} = e_{u_1} \cdots e_{u_r}$$

as $m \to \infty$. Thus, $\text{Sym}^{k-p^m} C_{0,\overline{T}}$ has basis $\{e_{u_1} \cdots e_{u_r} | i_1, \ldots, i_r \in \mathbb{Z}_{\geq 1}\}$ (with a hidden $e^{k-r}_{u_0}$ term in front of the $e_{u_1}$).

Hence, $\text{Sym}^{k-p^m} C_{0,\overline{T}}$ is a power series in $\{e_{u_1}, e_{u_2}, \ldots\}$.

For $E : C_{0,\overline{T}} \to C_{0,\overline{T}}$, we want to study $\text{Sym}^{k+p^m} E \to \text{Sym}^{k} E$ as $m \to \infty$. 45
Thus, \[ \text{Sym}^{k+p^n}(E)(\{e_{u_0}^{k-r}e_{u_{i_1}}\} \cdots i_r \in \mathbb{Z}_{\geq 1}) \rightarrow 0 \]

Now consider \( \{e_{u_1} \cdots e_{u_k} | i_1, \ldots, i_k \in \mathbb{Z}_{\geq 1} \} \). By definition,

\[ \text{Sym}^{k+p^n}(E)(e_{u_0}^{k-r}e_{u_{i_1}} \cdots e_{u_{i_r}}) = (Ee_{u_{i_1}}^{k-r})(Ee_{u_{i_1}}) \cdots (Ee_{u_{i_r}}) \]

where \( (Ee_{u_0})^{k+p^n-r} = (E(1))^{k+p^n-r} \). We will show, essentially, that \( E(1) = 1 + \pi \beta \), where \( \text{ord}_p(\beta) \geq 0 \). Since \( E(1)^{p^n} \rightarrow 1 \) as \( m \rightarrow \infty \), we should expect that \( (E(1))^{k+p^n-r} \rightarrow (E(1))^{k-r} \) as \( m \rightarrow \infty \).

Thus, \( \text{Sym}^{k+p^n}(E) \) has basis \( \{e_{u_1} \cdots e_{u_k} | i_1, \ldots, i_r \in \mathbb{Z}_{\geq 1} \} \) and

\[ (\text{Sym}^{k+p^n}(E)(e_{u_1} \cdots e_{u_k})) = (Ee_{u_0})^{k-r}(Ee_{u_{i_1}}) \cdots (Ee_{u_{i_k}}) \]

Notice that \( (Ee_{u_0})^{k-r} \) needs interpretation via the binomial expansion, but we will deal with that issue later.

So far, we specialized \( t \) to \( \bar{t} \) in \( f(t, x) \). Recall that

\[ f(t, x) = \sum_{u \in A} t_u x^u \in \mathbb{F}_p[\{t_u | u \in A\}, x_1^\pm, \ldots, x_n^\pm] \]

Let \( \Delta(f) \) = Newton polyhedron of \( f(t, x) \) with respect to \( x \in \mathbb{R}^n \) = convex hull of \( \{u \in A\} \cup \{0\} \).

\( \text{Cone}(\Delta) := \) all rays emanating from the origin through \( \Delta(f) \).

\( M(\Delta) := \mathbb{Z}^n \cap \text{Cone}(\Delta) \).

\( w : M(\Delta) \rightarrow \frac{1}{\beta} \mathbb{Z}_{\geq 0} \).

For notational convenience, \( M(\Delta) = M \).

24 Lecture 21 - Dillon

25 Lecture 22 - Brendan

26 Lecture 23 - Siegfred

In this lecture, we investigate the family\(^{29}\)

\[ f(t, x) = \sum_{u \in A} \tilde{t}_u x^u \]

of Laurent polynomials in \( \mathbb{F}_p[\tilde{t}_u : u \in A], x_1^\pm, \ldots, x_n^\pm \). Here, \( A \) is a subset of \( \mathbb{Z}^n \), and \( \tilde{t}_u \) is an element of \( \mathbb{F}_q^\times \) for each \( u \in A \). The letter \( t \) in \( f(t, x) \) stands for the set \( \{\tilde{t}_u : u \in A\} \). We are using multi-index notation for \( x \), i.e. \( x^u \) means \( x_1^{u_1} \cdot x_2^{u_2} \cdots \cdot x_n^{u_n} \), where \( u = (u_1, \ldots, u_n) \) in coordinate notation. The Laurent polynomial \( f(t, x) \), when considered as a Laurent polynomial in \( \mathbb{F}_p[\tilde{t}_u : u \in A][x_1^\pm, \ldots, x_n^\pm] \) with coefficients \( \tilde{t}_u \) and indeterminates \( x_1, \ldots, x_n \), gives rise to a Newton polytope\(^{30}\) \( \Delta \) in \( \mathbb{R}^n \). This Newton polytope in turn gives rise to \( \text{Cone}(\Delta) \) and \( M := M(\Delta) \). We define the “coefficient spaces”\(^{31}\)

\[ O_c := \left\{ \sum_{j \in \mathbb{Z}^{|A|}} c(j) \pi^{A^j} t^j \bigg| c(j) \in \mathbb{Z}[\pi^{1/\epsilon}], \ c(j) \rightarrow 0 \text{ as } |j| \rightarrow \infty \right\} \]

---

\(^{29}\)introduced in the 07Nov lecture

\(^{30}\)The Newton polytope, its cone, and the intersection \( M \) of the cone with \( \mathbb{Z}^n \) were all defined in the 26Sept lecture.

\(^{31}\)The developments in this lecture are similar to the developments in the 26Nov lecture. The main difference is the introduction of the parameter \( \epsilon \).
for \( e = 0, 1, 2, \ldots \). Here, we are using multi-index notation for \( t \), i.e. \( t^l \) means \( t_{u_1}^{i_1} t_{u_2}^{i_2} \cdots t_{u_{|A|}}^{i_{|A|}} \), where \( t_u \) denotes the Teichmüller representative of \( u \) for each \( u \in A \). The elements of \( A \) are denoted by \( u_1, \ldots, u_{|A|} \), and \( j = (j_1, \ldots, j_{|A|}) \) in coordinate notation. Also, \( \pi \) is \( ^{32} \pi \in \mathbb{Q}_p \) and, for each \( j \in \mathbb{Z}_{\geq 0}^{|A|} \), the integer \( |j| \) is defined to be the sum \( j_1 + \cdots + j_{|A|} \). For each \( \xi \in O_e \), define

\[
\deg(\xi) := \min \left\{ \frac{|j|}{p^e} : j \in \mathbb{Z}_{\geq 0}^{|A|}, c(j) \neq 0 \right\}.
\]

For each \( u \in M \), define the “filtration”

\[
O^{(u)}_e := \{ \xi \in O_e | \deg(\xi) \geq w(u) \}.
\]

Now define

\[
\mathcal{E}_0(O_e) := \left\{ \sum_{u \in M} C(u) x^u \mid C(u) \in O^{(u)}_e, \ C(u) \to 0 \ as \ w(u) \to \infty \right\}.
\]

For our immediate purposes, the condition\(^{33} \) that \( C(u) \to 0 \) as \( w(u) \to \infty \) is not necessary for now, but may be needed for further applications. The elements of \( \mathcal{E}_0(O_e) \) take the form\(^{34} \)

\[
\sum_{\substack{i \in \mathbb{Z}_{\geq 0}^{|A|} \\neq 0 \\leq |i|}} c(i, v) \pi^{\frac{|i|}{p^e}} t^i x^v,
\]

with \( c(i, v) \) nonzero only for \( \frac{|i|}{p^e} \geq w(v) \).

### Relative Frobenius

Recall the definition \( q = p^a \). We define\(^{35} \)

\[
F(t, x) := \prod_{u \in A} \theta(t_u x^u),
\]

where \( \theta \) is the \( \infty \)-splitting function\(^{36} \). Then\(^{37} \)

\[
F(t, x) = \sum_{i \in \mathbb{Z}_{\geq 0}^{|A|} \\neq 0 \\leq |i|} D(i, u) \pi^{\frac{|i|}{p^e}} t^i x^u,
\]

with \( \text{ord}_{p}(D(i, u)) \geq 0 \) and \( |i| \geq w(u) \). The condition \( |i| \geq w(u) \) means that the powers of \( t \) and \( x \) in the above power series expression for \( F(t, x) \) are related and are not independent of each other. Define the “relative Frobenius”\(^{38} \)

\[
\alpha(t) := \sigma^{-1} \circ \psi_{x,p} \circ F(t, x)
\]

and

\[
\alpha_0(t) := \psi_{x,q} \circ F_0(t, x)
\]

as maps from the sets \( \mathcal{E}_0(O_e) \). Here, \( \sigma \) is the element\(^{39} \) of \( \text{Gal}(\mathbb{Q}_q(\pi)/\mathbb{Q}_q(\pi)) \) such that \( \sigma(\pi) = \pi \) and \( \sigma(b) = b^{p^e} \) for Teichmüllers\(^{40} \); the map \( \psi_{x,p} \) is the Cartier operator\(^{41} \) with respect to \( x \); the map \( \psi_{x,q} \) is defined by \( \psi_{x,q} = \psi_{x,p}^q \); and the

\(^{32} \pi_{\infty} \) was defined in the 24Sept lecture.

\(^{33} \)In fact, this condition is superfluous in the definition. Indeed, we have \( |C(u)|_{p} \leq \max \{ |\pi|^{|i|/p^e} : c(j) \neq 0 \} \) by ultrametric inequality and the fact that the \( \text{ord}_{p} \)'s of the \( c(j) \)'s and the \( t_u \)'s are nonnegative. It follows that \( |C(u)|_{p} \leq |\pi|_{p}^{w(u)} \) for each \( u \in M \) because \( C(u) \in O^{(u)}_e \). Now \( |\pi|_{p}^{w(u)} \) tends to zero as \( w(u) \to \infty \) because \( \text{ord}_{p}(\pi) = \frac{1}{p^e-1} \) is positive. Thus we do not need to write “\( C(u) \to 0 \) as \( w(u) \to \infty \)” in the definition of \( \mathcal{E}_0(O_e) \).

\(^{34} \)Indeed, write \( C(v) = \sum_{i \in \mathbb{Z}_{\geq 0}^{|A|} \\neq 0 \\leq |i|} c(i, v) \pi^{\frac{|i|}{p^e}} t^i \) for each \( C(v) \) in \( \sum_{v \in M} C(v) x^v \in \mathcal{E}_0(O_e) \) and rearrange the sum. Since \( C(v) \in O^{(v)}_e \), it follows that \( c(i, v) \) is nonzero only when \( \frac{|i|}{p^e} \geq w(v) \).

\(^{35} \)Compare this with \( F(x) \) defined in the 03Oct lecture.

\(^{36} \)Defined in the 24Sept lecture

\(^{37} \)This was computed in the 26Nov lecture. If \( \theta(z) = \sum_{i=0}^{\infty} \theta_i z^i \), and \( i = (i_1, \ldots, i_{|A|}) \in \mathbb{Z}_{\geq 0}^{|A|} \), then \( D(i, u) = \theta_{i_1} \cdots \theta_{i_{|A|}} \pi^{-|i|} \) for \( u = i_1 u_1 + \cdots + i_{|A|} u_{|A|} \) and \( D(i, u) = 0 \) otherwise. Recall that, as proved in the 24Sept lecture, we have \( \text{ord}_{p}(\theta_i) \geq \frac{i}{p^e-1} \) for each \( i \). Thus, since \( \text{ord}_{p}(\pi) = \frac{1}{p^e-1} \), it follows that \( \text{ord}_{p}(D(i, u)) \geq 0 \) for each pair \( (i, u) \). The fact that \( w(u) \leq |i| \) for \( D(i, u) \neq 0 \) follows from the computation \( w(u) = w_1(i_1 u_1 + \cdots + i_{|A|} u_{|A|}) \leq i_1 w(u_1) + \cdots + i_{|A|} w(u_{|A|}) \leq |i|, \) where the last inequality follows from the fact that \( w(u_{|A|}) \leq 1 \) for each \( u_{|A|} \in A \).

\(^{38} \)These were also defined in the 26Nov lecture. Compare with the definitions of \( \alpha \) and \( \alpha_{0} \) in the 03Oct and 10Oct lectures.

\(^{39} \)More precisely, \( \sigma \) is constructed by lifting the Frobenius automorphism \( b \to b^p \) in \( \text{Gal}(F_q/F_p) \) to a generator \( \sigma \) of \( \text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) \) and then extending the domain of the generator to \( \mathbb{Q}_q(\pi) \) by defining \( \sigma(\pi) = \pi \). See the second paragraph in §2 of Adolphson, A. and Sperber, S.: \( \text{Newton polyhedra and the degree of the L-function associated to an exponential sum} \), Invent. Math. 88, 555-569 (1987).

\(^{40} \)The Teichmüllers in \( \mathbb{Q}_q(\pi) \) are the elements \( b \) of \( \mathbb{Q}_q \) with \( b^{p^e-1} = 1 \).

\(^{41} \)First defined in the 03Oct lecture
maps $F(t, x)$ and $F_a(t, x)$ from $E_0(O_x)$ mean multiplication by the power series $F(t, x)$ and $F_a(t, x)$, respectively. They are called “relative” because they depend on the parameter $t$. Now note that, for positive integer\(^2\) $N$,

$$\alpha(t^N) = \sigma^{-1} \circ \psi_{x, p} \circ F(t^N, x),$$

and recall that\(^3\)

$$\alpha_a(t) = \sigma(t^{p^{-1}}) \circ \cdots \circ \sigma(t) \circ \alpha(t).$$

**Proposition.** $\alpha \left( t^p \right)$ maps $E_0(O_t)$ into $E_0(O_{t+1})$.

**Proof.** Let $\xi \in E_0(O_t)$, so

$$\xi = \sum_{j \in \mathbb{Z}^{[A]}_{\geq 0}} c(j, v) \pi \frac{|j|}{p^v} t^j x^v,$$

with $|j|/p^v \geq w(v)$. Then (here, $p^v i$ is scalar multiplication of the vector $i$ by the scalar $p^v$)

$$(\sigma \circ \alpha \left( t^p \right))(\xi) = \psi_{x, p} \left( F(t^p, x) \cdot \xi \right)$$

$$= \psi_{x, p} \left( \sum_{i \in \mathbb{Z}^{[A]}_{\geq 0}} D(i, u) \pi p^{|i|} t^{|i|} x^u \cdot \sum_{j \in \mathbb{Z}^{[A]}_{\geq 0}} c(j, v) \pi \frac{|j|}{p^v} t^j x^v \right)$$

$$= \psi_{x, p} \left( \sum_{i, j, u, v} D(i, u) c(j, v) \pi \frac{|i| + |j|}{p^v} t^{i+j} x^{u+v} \right)$$

$$= \sum_{i, j, u, v} D(i, u) c(j, v) \pi \frac{|i| + |j|}{p^v} t^{i+j} x^{u+v}.$$

In the last sum, we define $x^{u+v}$ to be 0 if at least one coordinate of $u + v$ is not divisible by $p$. Rewrite the above so that we get a $p^0$ in the denominator of the exponent for $\pi$, and obtain

$$= \sum_{i, j, u, v} D(i, u) c(j, v) \pi \frac{|i| + |j|}{p^v} t^{i+j} x^{u+v}.$$

$$= \sum_{h \in \mathbb{Z}^{[A]}_{\geq 0}, h \in M} C(h, y) \pi \frac{|h|}{p^v} t^h x^y,$$

say, where

$$C(h, y) = C(h, y, \ell, \xi) : = \sum_{i, j, u, v} D(i, u) c(j, v) \pi \left( \frac{|i| + |j|}{p^v} \right) t^{i+j} x^{u+v},$$

with the sum over all $i, j \in \mathbb{Z}^{[A]}_{\geq 0}$ and $u, v \in M$ such that $p^v i + j = h$ and $\frac{1}{p^v} (u + v) = y$. To show that $(\sigma \circ \alpha \left( t^p \right))(\xi)$ is in $E_0(O_{t+1})$, it suffices to show that $C(h, y)$ satisfies three conditions: first, that $\text{ord}_p(C(h, y)) \geq 0$; second, that $C(h, y)$ is

\(^2\)We are using multi-index notation for $t^i$, i.e. $t^i$ means $t_{u_1}^{i_1} \cdots t_{u_{|A|}}^{i_{|A|}}$ for $i \in \mathbb{Z}^{[A]}_{\geq 0}$. However, if $N$ is a positive integer, then $t^N$ means $(t_{u_1}^{i_1} \cdots t_{u_{|A|}}^{i_{|A|}})^N$. Thus $F(t^N, x) = \prod_{u \in A, i} \theta(t_u^{N \cdot i_u} x^u)$.

\(^3\)This equation was proved in the 26Nov lecture. A similar proof was given in the 15Oct lecture. However, if one maintains the analogy between the case with parameter $t$ (as in the 26Nov lecture) and the case without the parameter $t$ (as in the 15Oct lecture), then $F_a(t, x)$, which was first defined in the 26Nov lecture, should have been defined as $\prod_{m=0}^{n-1} F^{x^m}(t^{p^m}, x^{p^m})$ in order for this equation to be true. Here, if $k$ is an integer and $m$ is a nonnegative integer then $F^{x^m}(t^{p^m}, x^{p^m})$ is defined by $\sum_{i, u} \sigma^k(D(i, u)) \pi \frac{|i|}{p^v} t^{i} x^{u}$, where $\sigma^k$ does not commute with the map $F(t^{p^m}, x^{p^m})$ defined by multiplication by $F(t^{p^m}, x^{p^m})$. Rather, we have $\sigma^k \circ F^{x^m}(t^{p^m}, x^{p^m}) = F^{x^m}(t^{p^m}, x^{p^m}) \circ \sigma^{-1}$ for integers $k$ and nonnegative integers $m$. Note that $\sigma^{-1}$ (and $\sigma$ as well) commutes with $\psi_{x, p}$, because $\psi_{x, p}$ only acts on the powers of $x$ and makes some coefficients zero. On the other hand, if $\sigma$ acts on power series of the form $\sum_{i, u} \sigma(c(i, u)) t^{i} x^{u}$, then we define $F^{x^m}(t^{p^m}, x^{p^m})$ by $\sum_{i, u} \sigma^k(D(i, u)) \pi \frac{|i|}{p^v} t^{i} x^{u}$. Note that $\sigma$ fixes $\pi$. This definition will then still give $\sigma^{-1} \circ F^{x^m}(t^{p^m}, x^{p^m}) = F^{x^m}(t^{p^m}, x^{p^m}) \circ \sigma^{-1}$ and guarantee that the equation expressing $\alpha_a$ in terms of $\alpha$ will hold.
nonzero only when \( \frac{|h|}{p^{\ell+1}} \geq w(y) \); and third, that \( C(h, y) \) tends to zero as \( |h| \to \infty \) for fixed \( y \). The first condition follows immediately from the definition of \( C(h, y) \) and the fact that the ord\(_p\)'s of the \( D(i, u) \) and \( c(j, v) \) and \( \pi \) are nonnegative. We know that \( D(i, u) \) is nonzero only when\(^{44} \) \( |i| \geq w(u) \), and \( c(j, v) \) is nonzero only when \( \frac{|j|}{p^{\ell}} \geq w(v) \). If \( C(h, y) \) is nonzero, then, in its sum definition, at least one quadruple \( i, j, u, v \) has both \( D(i, u) \) and \( c(j, v) \) nonzero. Thus, if \( C(h, y) \) is nonzero, then some \( i, j, u, v \) with \( p^\ell i + j = h \) and \( \frac{1}{p}(u + v) = y \) has \( |i| \geq w(u) \) and \( \frac{|j|}{p^{\ell}} \geq w(v) \). But this implies
\[
|h| = |p^\ell i + j| \\
= p^\ell |i| + |j| \\
\geq p^\ell w(u) + w(v)p^\ell \\
= p^\ell (w(u) + w(v)) \\
\geq p^\ell w(u + v) \\
= p^{\ell+1}w\left(\frac{u + v}{p}\right) \\
= p^{\ell+1}w(y).
\]

This gives that \( C(h, y) \) satisfies the second condition. Since each \( D(i, u) \) and each \( c(j, v) \) have ord\(_p\) nonnegative, it follows immediately from the definition of \( C(h, y) \) that it satisfies the third condition since \( |h| = p^\ell |i| + |j| \) and ord\(_p\)(\( \pi \)) > 0, so that \( \pi^{\left(\frac{|h|}{p^{\ell+1}}(p^\ell|i| + |j|)\right)} \) tends to 0 as \( |h| \to \infty \). Thus \( (\sigma \circ \alpha(p^\ell))(\xi) \) is in \( E_0(O_{t+1}) \). Hence \( \alpha(p^\ell)(\xi) \) is in \( E_0(O_{t+1}) \) since \( \sigma^{-1}(\xi) \in E_0(O_{t+1}) \) for \( 45 \xi \in E_0(O_{t+1}) \).

**Corollary.** \( \alpha_\sigma(t) \) maps \( E_0(O_0) \) into \( E_0(O_a) \).

**Proof.** We have
\[
\alpha_\sigma(t) = \alpha(t^{p^\ell-1}) \circ \cdots \circ \alpha(t^p) \circ \alpha(t).
\]

Now use the above proposition and induction on \( a \).

**Remark:** In the proof of the proposition, we showed that if \( \xi \in E_0(O_0) \), then (take \( \ell = 0 \) in the proof)
\[
(\sigma \circ \alpha(t))(\xi) = \sum_{i,j,u,v} D(i, u)c(j, v)\pi^{\left(\frac{|h|}{p^{\ell+1}}(|i| + |j|)\right)} \pi^{|i|+|j|} p^{\ell+1}i^j x^{\frac{n+1}{p}} y^x,
\]
which can be written as\(^{46} \)
\[
\sum_{\substack{h \in \mathbb{Z}_{\geq 0}^2 \\| y \in M \\| \\| \frac{|h|}{p} \geq w(y) \\| \}} \sum_{\xi \in E_0(O_0)} C(h, y, 0)\pi^{\frac{|h|}{p}} t^h x^y,
\]
with \( \frac{|h|}{p} \geq w(y) \) for each term, and with (as defined above)
\[
C(h, y, 0) = C(h, y, 0, \xi) = \sum_{i,j,u,v} D(i, u)c(j, v)\pi^{\left(\frac{|h|}{p^{\ell+1}}(|i| + |j|)\right)},
\]
with the sum over all \( i, j \in \mathbb{Z}_{\geq 0}^2 \) and \( u, v \in M \) such that \( i + j = h \) and \( \frac{1}{p}(u + v) = y \). Since each \( D(i, u) \) and \( c(j, v) \) has nonnegative ord\(_p\), we also have ord\(_p\)(\( C(h, y, 0) \)) \geq ord\(_p\) \( \left(\pi^{\frac{|h|}{p^{\ell+1}}(|i| + |j|)\right)} \), which equals \( |h|/p \) because ord\(_p\)(\( \pi \)) = \( \frac{1}{p^{\ell+1}} \).

**Symmetric Powers**

Denote \( x^u \) by \( e_u \) for each \( u \in M \). Write
\[
\alpha(t)(e_u) = \sum_{i \in \mathbb{Z}_{\geq 0}^2, v \in M} D(i, v)\pi^{\frac{|i|}{p}} t^i e_v,
\]

\(^{44}\) This was computed in the 26Nov lecture and also in a footnote above.

\(^{45}\) If we define the action of \( \sigma \) on \( \sum_{i,u} c(i, u)t^i x^u \) by \( \sum_{i,u} \sigma(c(i, u))t^i x^u \), then \( \xi \in E_0(O_{t+1}) \Rightarrow \sigma^{-1}(\xi) \in E_0(O_{t+1}) \) follows immediately from the fact that \( \sigma(h) \) has the same order as \( b \) for any \( b \in \mathbb{Q}_0(\pi) \). This suggests that the definition of the action of the map \( \sigma \) is \( \sigma : \sum_{i,u} c(i, u)t^i x^u \mapsto \sum_{i,u} \sigma(c(i, u))t^i x^u \), instead of \( \sigma : \sum_{i,u} c(i, u)t^i x^u \mapsto \sum_{i,v} c(i, u)t^i x^v \), since things are more complicated with the latter.

\(^{46}\) In the lecture we used the notation \( c^*(h, y) \) instead of \( C(h, y, 0) \).
where
\[ D(i, v) = D(i, v, e_u) := \sigma^{-1}(C(i, v, 0, e_u)), \]
so that, by the above remark, we have
\[ \text{ord}_p(D(i, v)) \geq \frac{|i|}{p} \geq w(v). \]
Also, setting \( u \) to be \((0, \ldots, 0)\), we have\(^{48}\)
\[ \alpha(t)(1) = 1 + \sum_{i,j,v} D(i, v, e_0)_{[n]} t^i e_v, \]
again with \( \text{ord}_p(D(i, v, e_0)) \geq \frac{|i|}{p} \geq w(v) \). Form the power series ring \( O_0[[\{e_u : u \in M\}]] \). Monomials in this set look like \( e_{u_1} \cdots e_{u_r} \). Define
\[ w : \prod_{i=1}^{\infty} M \to \frac{1}{D} \mathbb{Z}_{\geq 0} \cup \{\infty\} \]
by
\[ w(u) = \sum_{i=1}^{\infty} w(u_i), \quad \text{where} \ u = (u_1, u_2, \ldots), \]
and set \( M_\infty \) to be the set of all \( u \in \prod_{i=1}^{\infty} M \) such that \( w(u) \) is finite. Note that, since \( w(0) = 0 \) and the image of the weight function \( w \) is contained in \( \frac{1}{D} \mathbb{Z}_{\geq 0} \), it follows that \( M_\infty \) is the same as the set of all \( u = (u_1, u_2, \ldots) \) that have only finitely many nonzero coordinates \( u_\ell \). For \( u = (u_1, u_2, \ldots) \in M_\infty \) with \( u_\ell \neq 0 \) and \( u_\ell = 0 \) for \( \ell > r \), define
\[ e_u = e_{u_1} \cdots e_{u_r}. \]
Define \( e_{(0,0,\ldots)} \) to be 1. For each \( u \in M_\infty \), define
\[ O_\ell^u := \{ \xi \in O_\ell \mid \deg(\xi) \geq w(u) \}. \]
Define
\[ \text{Sym}^\infty E_0(O_\ell) := \left\{ \sum_{u \in M_\infty} c(u)e_u \middle| c(u) \in O_\ell^u, c(u) \to 0 \text{ as } w(u) \to \infty \right\}. \]
Note: \( \text{Sym}^\infty E_0(O_\ell) \) is a ring under formal addition and multiplication of power series\(^{49}\).

**Proposition.** If \( \underline{u} = (u_1, \ldots, u_r, 0, 0, \ldots) \in M_\infty \) and \( \gamma \in \mathbb{Z}_{\geq 0}^{|A|} \) with \( |\gamma| \geq w(u) \), then
\[ t^\gamma \cdot (\alpha(t)e_{u_1}) \cdots (\alpha(t)e_{u_r}) \in \text{Sym}^\infty E_0(O_1). \]

\(^{47}\) Again, here we are working under the assumption that the definition of the action of the map \( \sigma \) on power series is \( \sigma : \sum_{i,n} c(i, u)t^i u \to \sum_{i,n} \sigma(c(i, u))t^i u \).

\(^{48}\) Note that \( e_0 \) is just 1. Note also that \( D(0, 0, e_0) = C(0, 0, 0, e_0) = D(0, 0)c(0, 0) = D(0, 0) \cdot 1 = D(0, 0) = \theta_0 \cdots \theta_0 p^{-\beta} = 1 \) since \( \theta_0 = 1 \) by definition of \( \theta(z) \).

\(^{49}\) To show that \( \text{Sym}^\infty E_0(O_\ell) \) is closed under formal multiplication of power series, let \( C = \sum_{u \in M_\infty} c(u)e_u \) and \( D = \sum_{u \in M_\infty} d(u)e_u \) be elements of \( \text{Sym}^\infty E_0(O_\ell) \), so that \( c(u) = \sum_{j \in \mathbb{Z}_{\geq 0}^{|A|}} c(j, u)\pi^{[j]/p^j} t^j \) and \( d(u) = \sum_{j \in \mathbb{Z}_{\geq 0}^{|A|}} d(j, u)\pi^{[j]/p^j} t^j \) with \( c(j, u) \neq 0 \) nonzero only when \( [j]/p^j \geq w(u) \) and \( d(j, u) \neq 0 \) nonzero only when \( [j]/p^j \geq w(u) \). For \( u = (u_1, \ldots, u_r, 0, 0, \ldots) \) and \( v = (v_1, \ldots, v_s, 0, 0, \ldots) \in M_\infty \), define \( uv \) to be \( (u_1, u_2, \ldots, v_1, v_2, \ldots) \). Note that \( e_0e_u = e_u \) and that \( w(u) = w(uv) \). Then the product \( C \cdot D \) can be written as \( \sum_{y \in M_\infty} b(y)e_y \) with \( b(y) \) the (finite) sum of products \( c(y)d(y) \) such that \( uv = y \). Now \( c(y)d(y) = \sum_{k \in \mathbb{Z}_{\geq 0}^{|A|}} \left( \sum_{i+j=k} c(i, u)d(j, v) \right) \pi^{[k]/p^k} t^k \). If the coefficient \( \sum_{i+j=k} c(i, u)d(j, v) \) is nonzero then some pair \( i, j \) with \( i + j = k \) has both \( c(i, u) \neq 0 \) and \( d(j, v) \neq 0 \) nonzero; thus \( [k]/p^k \geq w(u) \) and \( [k]/p^k \geq w(v) \). Since \( i + j = k \), it follows that \( [k]/p^k \geq w(u) + w(v) = w(uv) \). Hence, in the product \( C \cdot D \), each \( b(y) \) is a sum of elements from \( O_\ell^u \), which implies \( b(y) \in O_\ell^u \). Now to show that \( b(y) \to 0 \) as \( w(y) \to \infty \), first note that \( c(u) \to 0 \) as \( w(u) \to \infty \) and \( d(y) \to 0 \) as \( w(y) \to \infty \) by definition of \( C \) and \( D \). Thus for each \( \varepsilon > 0 \) there is an \( A \) such that \( |c(y)|_p < \varepsilon \) for \( w(y) \geq A \) and \( |d(y)|_p < \varepsilon \) for \( w(y) \geq A \). If \( u + v = y \) and \( w(y) \geq 2A \), then \( (c(u) + c(v)) \to 0 \) as \( w(u) \to \infty \) and \( w(v) \to \infty \) by ultrametric inequality, because the terms in its expression as a sum have norm less than \( \varepsilon \). Hence \( b(y) \to 0 \) as \( w(y) \to \infty \), and the product \( C \cdot D \) is in \( \text{Sym}^\infty E_0(O_\ell) \). The proof that \( \text{Sym}^\infty E_0(O_\ell) \) is closed under formal addition of power series is similar (in fact more straightforward).
Proof. First note that, directly from the definitions, we have $E_0(O_1) \subseteq \operatorname{Sym}^\infty E_0(O_1)$ for each $\ell$ (because the elements in $E_0(O_{1})$ are sums over elements of $M_\infty$ that have all coordinates except the first equal to the zero element of $Z_{\geq 0}$). Write $\gamma$ as $\gamma_1 + \cdots + \gamma_r$ with $|\gamma_j| \geq w(u_j)$ for $j = 1, \ldots, r$. This is possible since $|\gamma| \geq w(u)$. Then
\[
t^\gamma \cdot (\alpha(t)e_{u_1}) \cdots (\alpha(t)e_{u_r}) = (\alpha(t)t^\gamma e_{u_1}) \cdots (\alpha(t)t^\gamma e_{u_r}).
\]
By the above proposition, since each $t^\gamma e_{u_j}$ is in $E_0(O_0)$, it follows that each $(\alpha(t)t^\gamma e_{u_j})$ is in $E_0(O_1)$. Hence the above product is in $\operatorname{Sym}^\infty E_0(O_1)$ since $\operatorname{Sym}^\infty E_0(O_1)$ is a ring.

27 Lecture 24 - Jamie

Let $k \in \mathbb{Z}_p$, define for each $e_{\underline{u}} = e_{u_1}e_{u_2} \cdots e_{u_r} = 1^{k-r}e_{u_1}e_{u_2} \cdots e_{u_r}$,
\[
(Sym^{\infty,k} \alpha(t))e_{\underline{u}} := (\alpha(t)e_{u_1})(\alpha(t)e_{u_2}) \cdots (\alpha(t)e_{u_r}).
\]
Note that $(\alpha(t)e_{u_1})(\alpha(t)e_{u_2})(\alpha(t)e_{u_r}) \in Sym^{\infty} E_0(O_1)$ by a proposition from last time.

**Proposition 27.1.** Let
\[
\xi = 1 + \sum_{\gamma \in \mathbb{Z}_{\geq 0}^{|A|}: \underline{u} \in M_\infty, (\gamma, \underline{u}) \neq 0} c(\gamma, \underline{u}) \pi^{\gamma |t^\gamma e_{\underline{u}}|} \in Sym^{\infty} E_0(O_0)
\]
Then $\xi^k \in Sym^{\infty} E_0(O_0)$ for all $k \in \mathbb{Z}_p$.

**Proof.** (Sketch) $\xi^k = (1 + \sum_{\gamma \in \mathbb{Z}_{\geq 0}^{|A|}} c(\gamma, \underline{u}) \pi^{\gamma |t^\gamma e_{\underline{u}}|})^k = \sum_{s=0}^{\infty} \binom{k}{s} \sum_{\gamma \in \mathbb{Z}_{\geq 0}^{|A|}} c(\gamma, \underline{u})^{s \gamma |t^\gamma e_{\underline{u}}|}$. You can show that this infinite sum of elements in $Sym^{\infty} E_0(O_0)$ converges.

**Remark.**

1. The same proposition holds if $O_0$ is replaced by $O_1$.

2. If $\operatorname{ord}_p(c(\gamma, \underline{u})) = \frac{|\gamma|}{p^r}$ then the same holds true for $\xi^k$. (If $\xi^k \sum c'(\gamma', \underline{u}')\pi^{\gamma' |t^\gamma e_{\underline{u}}|}$ then $\operatorname{ord}_p(c'(\gamma', \underline{u}')) \geq \frac{|\gamma'|}{p^r}$.)

As a consequence,

**Proposition 27.2.** $Sym^{\infty,k} \alpha(t) : Sym^{\infty} E_0(O_0) \rightarrow Sym^{\infty} E_0(O_1)$ is well defined.

**Corollary 27.3.** $Sym^{\infty,k} \alpha(t) : Sym^{\infty} E_0(O_0) \rightarrow Sym^{\infty} E_0(O_k)$.

**Definition 27.4.** Define the Cartier operator, $\psi_{i,p}$, for $i \in \mathbb{Z}_{\geq 1}$
\[
\psi_{i,p} : Sym E_0(O_{1+i}) \otimes \bigwedge^i E_0(O_{1+i}) \rightarrow Sym E_0(O_1) \otimes \bigwedge^i E_0(O_1)
\]
by
\[
\psi_{i,p} : t^\gamma e_{\underline{u}} \otimes e_v \mapsto t^{\gamma/p} e_{\underline{u}} \otimes e_v
\]
where $e_v = e_{v_1} \wedge \cdots \wedge e_{v_i}$ (and where $t^{\gamma/p}$ is replaced by 0 if $p \not| \gamma$).

For each $i \geq 1$ define $\beta^{(k,i)} := \psi_{i,p} \circ Sym^{\infty,k-i} \alpha(t) \otimes \bigwedge^i \alpha(t)$, and this is an endomorphism of $Sym^{\infty} E_0(O_0) \otimes \bigwedge^i E_0(O_0)$.

**Proposition 27.5.** The matrix of $\beta^{(k,i)}$ with respect to $B_i$ is $(B_i(\gamma, \underline{u}, \gamma', \underline{v}, \gamma'', \underline{w}))$ with $\operatorname{ord}_p(B_i(\gamma, \underline{u}, \gamma', \underline{v}, \gamma'', \underline{w})) \geq |\gamma'|$. 

**Proof.**
Let \( \beta \) be an (orthonormal) basis of \( H \). Last time we estimated the ord of entries in the matrix of

\[
\begin{pmatrix}
\psi_{1,p} \circ \text{Sym}^k \alpha(t) \\
\wedge \alpha(t)
\end{pmatrix}
\]

The same proof shows that

\[
(\text{The matrix of } [\beta]_k \text{ wrt } B) = (B_{(\gamma, \hat{u}, \hat{v}), (\gamma', \hat{u}', \hat{v}')} )
\]

satisfies

\[
\text{ord}_p (B_{(\gamma, \hat{u}, \hat{v}), (\gamma', \hat{u}', \hat{v}')} ) \geq |\gamma'|.
\]

Now define \( w(N) := \# \{ \pi^{ |\gamma|/p^r } \gamma e_u \otimes e_v \in B \mid |\gamma| = N \} \). (Note: \( w(N) < \infty \) by construction) The \( p \)-adic newton polygon of \( \det(1 - [\beta]_k T) \) lies on or above the lower convex hull of the points

\[
\left( \sum_{N=1}^\ell w(N), \sum_{N=1}^\ell N \cdot w(N) \right)
\]

for \( \ell = 0, 1, 2, \cdots \). As a consequence we get that \( \det(1 - [\beta]_k T) \) is \( p \)-adic entire. Define \( \psi_{t,q} := (\psi_{t,p})^a \) (where \( q = p^a \)) and

\[
[\beta_a]_k := \psi_{t,q} \circ [\alpha_a(t)]_k : H_0 \to H_0
\]

an endomorphism of \( H_0 \).

**Proposition 28.1.** \([\beta_a]_k = ([\beta]_k)^a\). (Compare with \( \alpha_a = \alpha^a \) from long ago...)

Using methods similar to before we get
Proposition 28.2. The $q$-adic Newton polygon of $\det(1 - [\beta_a]_k T)$ lies on or above the lower convex hull of the points

$$\left( \sum_{N=1}^{\ell} w(N), \sum_{N=1}^{\ell} N \cdot w(N) \right)$$

for $\ell = 0, 1, 2, \cdots$ and hence $\det(1 - [\beta_a]_k T)$ is $p$-adic entire.

Our goal is to show for $k \in \mathbb{Z}_p$

$$L_{\text{unit}}(k, T) := \prod_{t \in [\mathbb{Z}_p]/\mathbb{Z}_p} \frac{1}{1 - \pi_0(\hat{t})^k T^{\deg(t)}} = \det(1 - [\beta_a]_k T)^{\delta[A]}$$

and hence the unit root $L$-function is $p$-adic meromorphic.

Proposition 28.3. (Durok trace formula)

For all $m \geq 1$,

$$(q^m - 1)^{|A|} \Tr \left( ([\beta_a]_k)^m \right) = \sum_{t^m-1=1} \Tr \left( \alpha_a(\hat{t} q^{m-1}) \circ \cdots \circ \alpha_a(\hat{t}) \circ \alpha_a(\hat{t}) \right)$$

We define the notation $\alpha_{a,m}(t) := \alpha_a(\hat{t} q^{m-1}) \circ \cdots \circ \alpha_a(\hat{t}) \circ \alpha_a(\hat{t})$ and thus

$$(q^m - 1)^{|A|} \Tr \left( ([\beta_a]_k)^m \right) = \sum_{t^m-1=1} \Tr \left( [\alpha_{a,m}(t)]_k \right)$$

(Compare this with our original Durok trace formula:)

$$(q^m - 1)^n \Tr(\alpha^m_a) = \sum_{\hat{t}^m-1=1} F(\hat{t} q^{m-1}) \circ \cdots \circ F(\hat{t} q) \circ F(\hat{t})$$

We then compute,

$$\det(1 - [\beta_a]_k T)^{\delta[A]} = \exp \left( \sum_{m=1}^{\infty} (q^m - 1)^{|A|} \Tr \left( ([\beta_a]_k)^m \right) \frac{T^m}{m} \right)$$

$$= \exp \left( \sum_{m=1}^{\infty} \sum_{t^m-1=1} \Tr \left( [\alpha_{a,m}(\hat{t})]_k \right) \frac{T^m}{m} \right)$$

$$= \exp \left( \sum_{r=1}^{\infty} \sum_{t \in (\mathbb{F}_q)^{|A|}} \sum_{s=1}^{\infty} \sum_{t^m-1=1} \Tr \left( [\alpha_{a,s}(\hat{t})]_k \right) \frac{T^m}{m} \right)$$

$$= \prod_{t \in (\mathbb{F}_q)^{|A|}} \exp \left( \sum_{s=1}^{\infty} \Tr \left( [\alpha_{a,s}(\hat{t})]_k \right) \frac{T^s}{s} \right)$$

Claim 1: $\alpha_{a,sd}(\hat{t}) = \left( \alpha_{ad}(\hat{t}) \right)^s$

Claim 2: $[\alpha(t)^*]_k = \left( \alpha(t) \right)^s$

Claim 3: $\det(1 - [\alpha_{ad}(\hat{t})]_k T^{\delta(\hat{t})}) = 1 - \pi_0(\hat{t})^k T$

and thus the above equals

$$\cdots = \prod_{t} \exp \left( \sum_{s=1}^{\infty} \Tr \left( [\alpha_{ad}(\hat{t})]_k \right)^s \frac{T^s}{s} \right)$$

$$= \prod_{t} \exp \left( \sum_{s=1}^{\infty} \Tr \left( \left( [\alpha_{ad}(\hat{t})]_k \right)^s \right) \frac{T^s}{s} \right)$$

$$= \prod_{t} \left( \det(1 - [\alpha_{ad}(\hat{t})]_k T^{\delta(\hat{t})}) \right)^{\frac{1}{\left| (\mathbb{F}_q)^{|A|} \right|}}$$

$$= L_{\text{unit}}(k, T)$$

To complete the proof we must prove the three claims.
29 Lecture 26 - Meg

Claim.

\[
\det \left( 1 - [\alpha_{ad(\tilde{t})}] k T \right) = 1 - \pi_0(\tilde{t})^k T
\]

Proof. (Sketch)

Set \( w(\tilde{u}, \tilde{v}) := w(\tilde{u}) + w(\tilde{v}) \). Define

\[
\mathcal{H}_c(\tilde{t}) = \left\{ \sum_{\tilde{u},\tilde{v} \in \mathcal{M}_{\infty} \setminus \{0\}} c(\tilde{u}, \tilde{v}) \pi^w(\tilde{u}, \tilde{v}) e_{\tilde{u}} \otimes e_{\tilde{v}} : c(\tilde{u}, \tilde{v}) \in \mathbb{Z}_{\geq 1}[1/p^\gamma], c(\tilde{u}, \tilde{v}) \to 0 \text{ as } w(\tilde{u}, \tilde{v}) \to \infty \right\}
\]

There is a map \( \mathcal{H}_c \to \mathcal{H}_c(\tilde{t}) \) where \( \pi^{\gamma/\gamma^\prime} \tau^\gamma e_{\tilde{u}} \otimes e_{\tilde{v}} \mapsto \pi^{\gamma/\gamma^\prime} (1 - w(\tilde{u}, \tilde{v})) \tau^\gamma \). We then have the following commutative diagram.

\[
\begin{array}{ccc}
\mathcal{H}_0 & \xrightarrow{\alpha_{ad(\tilde{t})}} & \mathcal{H}_0(\tilde{t}) \\
\downarrow^{\alpha_{ad(\tilde{t})}} & & \downarrow^{\alpha_{ad(\tilde{t})}} \\
\mathcal{H}_{ad(\tilde{t})} & \xrightarrow{\alpha_{ad(\tilde{t})}} & \mathcal{H}_{ad(\tilde{t})}(\tilde{t})
\end{array}
\]

Fix \( k \in \mathbb{Z}_{\geq 1} \). Recall (from long ago),

\[
\text{Sym}^{k-i} C_{0,7} \otimes \Lambda^i C_{0,7} \xrightarrow{\text{embed}} \mathcal{H}_0(\tilde{t})
\]

where

\[
\pi^* e_{u_1} \otimes \cdots \otimes e_{u_{k-i}} \otimes e_{v_1} \wedge \cdots \wedge e_{v_i} \mapsto \pi^* e_{u_{k-i}} \otimes \cdots \otimes e_{u_1} \otimes e_{v_1} \wedge \cdots \wedge e_{v_i}
\]

Next, \( \text{Sym}^{k-i} \alpha_{ad(\tilde{t})} \otimes \Lambda^i \alpha_{ad(\tilde{t})} \) acts on \( \text{Sym}^{k-i} C_{0,7} \otimes \Lambda^i C_{0,7} \), but can be viewed as an operator on the embedded space in \( \mathcal{H}_0(\tilde{t}) \) by

\[
(\text{Sym}^{k-i} \alpha \otimes \Lambda^i \alpha)(e_{u_1} \otimes \cdots \otimes e_{u_{k-i}} \otimes e_{v_1} \wedge \cdots \wedge e_{v_i}) = (\alpha e_0)^{k-i-r}(\alpha e_{u_1}) \cdots (\alpha e_{u_{k-i}}) \otimes (\alpha e_{v_1}) \wedge \cdots \wedge (\alpha e_{v_i})
\]

Define

\[
E_k(\tilde{t}) := \bigoplus_{i=0}^k (-1)^{i-1}(i-1)\text{Sym}^{k-i} \alpha \otimes \Lambda^i
\]

is an operator on

\[
\mathcal{H}_0(\tilde{t})
\]

a subspace of \( \mathcal{H}_0(\tilde{t}) \). Extend \( E_k(\tilde{t}) \) to an operator on \( \mathcal{H}_0(\tilde{t}) \) by

\[
E_k(\tilde{t}) x = \begin{cases} E_k(\tilde{t}) x & \text{if } x \in \bigoplus_{i=0}^k \mathcal{H}_0(\tilde{t})^{(k,i)} \\ 0 & \text{otherwise} \end{cases}
\]

Technically, we need to show that \( E_{k+p^m}(\tilde{t}) \) converges to \( [\alpha_{ad(\tilde{t})}] k \) as operators, but we will not do this due to time constraints. Consequently,

\[
\det(1 - E_{k+p^m}(\tilde{t}) T) \to \det(1 - [\alpha_{ad(\tilde{t})}] k T)
\]

as \( m \to \infty \), meaning the coefficients of \( \det(1 - E_{k+p^m}(\tilde{t}) T) \) tend to the coefficients of \( \det(1 - [\alpha_{ad(\tilde{t})}] k T) \).

A while back, we showed that

\[
\det(1 - \alpha_{ad(\tilde{t})}^k T) = \det(1 - E_k(\tilde{t}) T) = \prod_{i=1}^\infty (1 - \pi_i(\tilde{t})^k T)
\]

and

\[
\text{Tr}(\alpha_{ad(\tilde{t})}^k) = \sum_{i=1}^k (-1)^{i-1}(i-1) \text{Tr}(\text{Sym}^{k-i} \alpha_{ad(\tilde{t})} \otimes \Lambda^i \alpha_{ad(\tilde{t})}) = \text{Tr}(E_k(\tilde{t}))
\]

so

\[
\lim_{m \to \infty} \det(1 - E_{k+p^m}(\tilde{t}) T) = \lim_{m \to \infty} \prod_{i=1}^\infty (1 - \pi_i(\tilde{t})^{k+p^m} T) = (1 - \pi_0(\tilde{t})^k T)
\]

since \( \pi_i(\tilde{t}) \) has \( \text{ord}_p > 0 \) except for \( \text{ord}_p(\pi_0) = 0 \).