18.758 Supplementary Notes
February 22, 2005

Exponential and logarithm in p-adic fields

Suppose F is a finite extension of $\mathbb{Q}_p$, say of degree m. Write

$$\mathcal{O} = \text{ring of integers in } F = \{x \in F \mid |x|_F \leq 1\}$$

$$\mathfrak{m} = \text{maximal ideal in } \mathcal{O} = \{x \in F \mid |x|_F < 1\}$$

$$q = |\mathcal{O}/\mathfrak{m}| = p^f = \text{smallest norm bigger than 1 of an element of } F.$$

The positive integer f is the *residue class degree*, the degree of the field extension $\mathcal{O}/\mathfrak{m} \subset \mathbb{Z}_p/p\mathbb{Z}_p$.

We have $|p|_F = p^{-m}$ since multiplication by p on the m-dimensional $\mathbb{Q}_p$-vector space F must dilate the Haar measure by p^{-m}. On the other hand, the norm of p must be a (negative) power of q; we write

$$|p|_F = q^{-e},$$

with e a positive integer called the *ramification index* of F over $\mathbb{Q}_p$. It follows that $m = ef$. In fact f is the degree of the largest unramified (over $\mathbb{Q}_p$) subfield E of F.

I stated in class that the elements of $(\mathcal{O}/\mathfrak{m})^\times$ lift to $\mathcal{O}^\times$ as $(q-1)$st roots of unity, and that these are precisely the roots of 1 of order prime to p in F. More specifically,

$$E = \mathbb{Q}_p[(q-1)\text{st roots of unity}] \subset F$$

Obviously none of these roots of unity (except 1) belongs to $1 + \mathfrak{m}$.

I want to see when the exponential and logarithm functions are defined, using their standard power series expansions

$$\exp t = \sum_{n=0}^{\infty} t^n/n!, \qquad \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} x^n/n.$$

We have formal power series identities

$$\exp(t+s) = \exp(t)\exp(s), \qquad \log[(1+x)(1+y)] = \log(1+x) + \log(1+y)$$

$$\log(\exp(t)) = t, \qquad \exp(\log(1+x)) = 1 + x;$$

these will be identities in F whenever the series converge.

A series in F converges if and only if its terms tend to zero (because of the ultrametric inequality $|a+b|_F \leq \max\{|a|_F, |b|_F\}$). So we need to estimate the norms of the coefficients.

Lemma 1. *For $n \geq 1$,*

$$|1/n!|_F = q^{e\left([n/p]+[n/p^2]+\cdots\right)} \leq q^{e(n/p)(1/(1-p^{-1}))} = q^{ne/(p-1))}.$$

Here $[x]$ is the greatest integer less than or equal to x.

Lemma 2. *The series* $\exp(t)$ *converges for*

$$|t|_F < q^{-e/(p-1)};$$

equivalently, for $t \in \mathfrak{m}^N$ *whenever* $N > \frac{e}{p-1}$*. In this case,*

$$\exp(\mathfrak{m}^N) = 1 + \mathfrak{m}^N.$$

To get the last equality (as opposed to containment), we use the fact that the first non-constant term in the series is larger than all later terms.

The logarithm series converges better.

Lemma 3. *For* $n \geq 1$*,*

$$|1/n|_F \leq n^m,$$

with equality exactly when n *is a power of* p*. Consequently the series* $\log(1+x)$ *converges for* $x \in \mathfrak{m}$*.*

The reason is that

$$|x^n/n|_F \leq n^m q^{-n},$$

and the exponential decay of q^{-n} is faster than the polynomial growth of n^m.

In order to see exactly where log takes values, we need to estimate these terms more precisely.

Lemma 4. *Suppose* $N > \frac{e}{p-1}$*, and* $x \in \mathfrak{m}^N$*. Then the first term in the series for* $\log(1+x)$ *is strictly larger than all successive terms. Consequently* log *is a bijection*

$$1 + \mathfrak{m}^N \to \mathfrak{m}^N.$$

Its inverse is exp*.*

Proof. We claim first of all that

$$|x^n/n|_F < |x^p/p|_F \qquad (n > p). \tag{1}$$

Here is a proof. According to Lemma 3,

$$|x^n/n|_F \leq n^m q^{-nN},$$

with equality exactly when n is a power of p. The function $n^m q^{-nN}$ increases from $n = 0$ to $n_0 = m/N \log q$, and then decreases. The maximum satisfies

$$n_0 = m/(Nf \log p) = e/N \log p < (p-1)/\log p < p;$$

this last inequality is equivalent to $\log p > 1 - 1/p$, which is trivial for $p \geq 3$ and easy to check for $p = 2$. Now (1) follows.

On the other hand, we have

$$|x^n/n|_F = |x|_F^n < |x|_F \qquad (1 < n < p). \tag{(2)}$$

From (1) and (2) we see that the largest term in the log series is either the first or the pth. But

$$|x^p/p|_F/|x|_F = |x|_F^{p-1}|p|_F^{-1} = |x|_F^{p-1} \cdot q^e \leq q^{-N(p-1)+e}.$$

The hypothesis on N is exactly that this last exponent is strictly negative; so the first term is strictly the largest. $\square$