1 Revision

Proposition 1.1 (Cor. 1.4 in Talk 8)**.** *If $a_n \in \mathbb{Q}_p$, then the series $\sum a_n$ is convergent if and only if $\lim_{n\to\infty} a_n = 0$, which implies $|\sum a_n| \le \max_n |a_n|$.*

Proposition 1.2 (Prop. 1.5 in Talk 8)**.** *Let $b_{ij} \in \mathbb{Q}_p$ and suppose that $\forall \varepsilon > 0\ \exists N = N(\varepsilon) : \max\{i,j\} \ge N \implies |b_{ij}| < \varepsilon$, then both series $\sum_{i\ge 0}\left(\sum_{j\ge 0} b_{ij}\right)$ and $\sum_{j\ge 0}\left(\sum_{i\ge 0} b_{ij}\right)$ converge and have equal sum.*

Proposition 1.3 (Prop. 2.1 in Talk 8)**.** *Let $f(X) \in \mathbb{Q}_p[[X]]$ be a power series, then the radius of convergence is $\rho = \left(\limsup_{n\to\infty} \sqrt[n]{|a_n|}\right)^{-1}$.*

2 Formal Derivatives of Power Series

Definition 2.1. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$, we define its **formal derivative** as

$$f'(X) = \sum_{n\ge 1} n a_n X^{n-1},$$

Theorem 2.2. *Let $f(X) = \sum a_n X^n$, $f'(X)$ its formal power series,then $f'(X)$ has the properties of the derivative:*

- *Additivity:* $(f+g)'(X) = f'(X) + g'(X)$

  Proof.
  $$(f+g)'(X) = (\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n)' = (\sum_{n=0}^{\infty}(a_n+b_n)X^n)' =$$
  $$\sum_{n=1}^{\infty} n(a_n+b_n)X^{n-1} = \sum_{n=1}^{\infty} n a_n X^{n-1} + \sum_{n=1}^{\infty} n b_n X^{n-1} = f'(X) + g'(X)$$
  □

- *Product Rule:* $(fg)'(X) = f(X)g'(X) + f'(X)g(x)$

  Proof.
  $$f(X)g'(X) + f'(X)g(X) = \left(\sum_{n=0}^{\infty} a_n X^n\right)\cdot\left(\sum_{n=0}^{\infty}(n+1)b_{n+1}X^n\right) + \left(\sum_{n=0}^{\infty}(n+1)a_{n+1}X^n\right)\cdot\left(\sum_{n=0}^{\infty} b_n X^n\right)$$
  $$= \sum_{n=0}^{\infty} c_n X^n + \sum_{n=0}^{\infty} d_n X^n, \quad c_n = \sum_{i=0}^{n}(i+1)b_{i+1}a_{n-i}, d_n = \sum_{i=0}^{n}(i+1)a_{i+1}b_{n-i}$$
  $$= \sum_{n=0}^{\infty}\sum_{i=0}^{n}(i+1)b_{i+1}a_{n-i}X^n + \sum_{n=0}^{\infty}\sum_{i=0}^{n}(i+1)a_{i+1}b_{n-i}X^n = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n}(i+1)b_{i+1}a_{n-i} + \sum_{i=0}^{n}(i+1)a_{i+1}b_{n-i}\right)X^n$$
  $$= \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n}(i+1)(b_{i+1}a_{n-i} + a_{i+1}b_{n-i})\right)X^n$$
  □

- *Chain Rule:* $(f\circ g)'(X) = f'(g(X))g'(X)$

  Proof. □

Proposition 2.3. *Let $f(X)$ be a power series which converges for all $|x| < \rho$, if $|a| < 1$ and $|b| < \rho$, then $g(x) = f(ax+b)$ is given by a power series $g(X)$ which converges for $|x| < \rho$.*

Proof. Since $|a| = |1|$ and $|b| < \rho$, we get

$$|ax+b| \le \max\{|x|, |b|\} < \rho \iff |x| \le b < \rho.$$

Now let $f(X) = \sum_{n\ge 0} c_n X^n$, we want to write $g(X)$ as a power series

$$g(x) = f(ax+b) = \sum_{n\ge 0} c_n(ax+b)^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n} c_n \binom{n}{k} a^k b^{n-k} x^k$$

Define

$$\alpha_{kn} = \begin{cases} \binom{n}{k} c_n a^k b^{n-k} x^k, & k \le n \\ 0 & k > n \end{cases} \implies \lim_{k\to\infty} |\alpha_{kn}| = 0$$

$$|\alpha_{kn}| = \left|\binom{n}{k} c_n a^k b^{n-k} x^k\right| \le \left|c_n b^n \left(\frac{x}{b}\right)^k\right| = |c_n b^n| \cdot \left|\left(\frac{x}{b}\right)^k\right| \le |c_n b^n| \max(1, \left|\frac{x}{b}\right|^n) \le \max(|c_n b^n|, |c_n x^n|)$$

Since $|x| < \rho, |b| < \rho$ we know that $\sum c_n x^n$ and $\sum c_n b^n$ converge $\iff$ $\lim_{n\to\infty} |c_n x^n| = \lim_{n\to\infty} |c_n b^n| = 0 \implies \lim_{n\to\infty} \alpha_{kn} = 0$. So using Proposition 1.2 we get

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n} c_n \binom{n}{k} a^k b^{n-k} x^k = \sum_{k=0}^{\infty}\sum_{n=k}^{\infty} c_n \binom{n}{k} a^k b^{n-k} x^k = \sum_{k\ge 0} \left(\sum_{n\ge k} \binom{n}{k} c_n a^k b^{n-k}\right) x^k =: g(x).$$

□

Proposition 2.4. *Let $f(X)$ be a power series with radius of convergence ρ, $f'(X)$ its formal derivative, and ρ' its radius of convergence, then $\rho' \ge \rho$.*

Proof. Let $f(X) = \sum a_n X^n, f'(X) = \sum_{n\ge 1} n a_n X^{n-1}$, then by Prop. 1.3 the radius of convergence of $f'(X)$ must be

$$\rho' = \left(\limsup_{n\to\infty} \sqrt[n]{\|n a_n\|}\right)^{-1} \ge \left(\limsup_{n\to\infty} \sqrt[n]{\|a_n\|}\right)^{-1} = \rho$$

□

Corollary 2.5. *Suppose $f(X)$ and $g(X)$ are power series which converge for $|x| < \rho$. If $f'(x) = g'(x)$ for all $|x| < \rho$, then there exists some $c \in \mathbb{Q}_p$ with $f(X) = g(X) + c$.*

Proof. Let $f(X) = \sum a_n X^n, g(X) = \sum b_n X^n$ and $f'(X), g'(X)$ their respective formal derivatives. We know that whenever $|x| < \rho$ we have

$$\sum_{n\ge 1} n a_n x^{n-1} = \sum_{n\ge 1} n b_n x^{n-1} \implies a_n = b_n \forall n \ge 1 \implies f(X) = g(X) + c$$

□

3 Strassman's Theorem

Theorem 3.1 (Strassman)**.** *Let $f(X) \in \mathbb{Q}_p[[X]]$ and suppose we have $\lim_{n\to\infty} a_n = 0$, so that $f(x)$ converges $\forall x \in \mathbb{Z}_p$. Define $N \in \mathbb{N}_0$ by the following conditions*

$$|a_N| = \max_{n\in\mathbb{N}_0} |a_n| \text{ and } |a_n| < |a_N|, \forall n > N$$

then the function f has at most N zeros.

Proof. induction on N.

- Base case: if $N = 0$, then $|a_0| > |a_n|, \forall n \ge 1$, we want to show that there are no zeros: $f(x) \ne 0 \forall x \in \mathbb{Z}_p$, if we had $f(x) = 0$, then

$$0 = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$
$$\implies |a_0| = |a_1 x + a_2 x^2 + \cdots| \le \max_{n\ge 1} |a_n x^n| \le \max_{n\ge 1} |a_n|$$

  But this contradicts the assumption that $|a_0| > |a_n|, \forall n \ge 1$, so there are no zeros in this case.

- Induction step: Suppose N was defined like before, and $\exists \alpha \in \mathbb{Z}_p : f(\alpha) = 0$, then we have for any $x \in \mathbb{Z}_p$

$$f(x) = f(x) - f(\alpha) = \sum_{n=0}^{\infty} a_n x^n - \sum_{n=0}^{\infty} a_n \alpha^n = \sum_{n=0}^{\infty} a_n (x^n - \alpha^n) \overset{2.1}{=} (x - \alpha) \sum_{n=0}^{\infty}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}$$

$$= (x - \alpha) \sum_{n=0}^{\infty}\sum_{j=0}^{\infty} c_{nj}, \quad c_{nj} := \begin{cases} a_n x^j \alpha^{n-1-j} & j < n, \\ 0 & j \ge n. \end{cases}$$

  We can use Proposition 1.2 to change the order of the summation but first we have to show the conditions of the proposition:

  1. $\forall n \in \mathbb{N}_0, \lim_{j\to\infty} c_{nj} = 0$: Clear, since we have $c_{nj} = 0, \forall j \ge n$.
  2. $\lim_{n\to\infty} c_{nj} = 0$ uniformly in j: This is also easy to see, because we have $|a_n x^j \alpha^{n-1-j}| \le |a_n| \to 0$ unrelated to j.

So we can switch the sums and then we have

$$(x-\alpha)\sum_{n=0}^{\infty}\sum_{j=0}^{\infty} c_{nj} = (x-\alpha)\sum_{j=0}^{\infty}\sum_{n=0}^{\infty} c_{nj}$$

since $\forall j \geq n : c_{nj} = 0$, we need to only consider when $n > j$ so its equal to

$$= (x-\alpha)\sum_{j=0}^{\infty}\sum_{n=j+1}^{\infty} a_n x^j \alpha^{n-1-j} = (x-\alpha)\sum_{j=0}^{\infty} x^j \underbrace{\sum_{n=0}^{\infty} a_{n+j+1}\alpha^n}_{=:b_j}$$

$$= (x-\alpha)g(x), \quad g(x) := \sum_{j=0}^{\infty} b_j x^j$$

Now we check if $g(X)$ fits the assumptions of the theorem, to use the induction steps. We need to show that $g(X)$ is non zero and that $b_j \to 0$

- $g(X)$ is non zero: clear since if $g(X)$ was the zero power series then $f(X)$ would also be zero, which is a contradiction.
- $b_j \to 0$: Consider $|b_j| = |\sum_{n=0}^{\infty} a_{n+j+1}\alpha^n| \leq \max_n |a_{n+j+1}\alpha^n| \leq \max_n |a_{n+j+1}| \xrightarrow{j\to\infty} 0$

Now we look for $\max_j |b_j|$, note that

$$|b_j| \leq \max_n |a_{n+j+1}| \leq |a_N|, \forall j$$

So we have

$$|b_{N-1}| = \left|\sum_{n=0}^{\infty} a_{N+n}\alpha^n\right| = \left|a_N + \sum_{n=1}^{\infty} a_{N+n}\alpha^n\right|$$

By 1.3 we have

$$\left|\sum_{n=1}^{\infty} a_{N+n}\alpha^n\right| \leq \max_{n\geq 1} |a_{N+n}| < a_N$$

$$\implies |a_N| \neq \left|\sum_{n=1}^{\infty} a_{N+n}\alpha^n\right| \implies \left|a_N + \sum_{n=1}^{\infty} a_{N+n}\alpha^n\right| \overset{\text{Prop 2.2}}{=} \max\left\{|a_N|, \left|\sum_{n=1}^{\infty} a_{N+n}\alpha^n\right|\right\} = |a_N| = |b_{N-1}|$$

Finnaly, if $j > N-1$, then

$$|b_j| \leq \max_k |a_{j+k+1}| \leq \max_{j>N} |a_j| < |a_N| = |b_{N-1}|$$

So the index at which the maximum coefficient b_n is reached is $N-1$, if we assume that $g(X)$ has at most $N-1$ zeros in $\mathbb{Z}_p$ then $f(X)$ has at most N zeros (g's zeros and α), this proves the theorem.

□

Corollary 3.2. *Let $f(X) = \sum a_n x^n$ be a non-zero power series which converges on $\mathbb{Z}_p$, and let $\alpha_1, ..., \alpha_m \in \mathbb{Z}_p$ be the roots of $f(X)$ in $\mathbb{Z}_p$, then there exists another power series $g(X)$ which also converges on $\mathbb{Z}_p$ but has no zeros in $\mathbb{Z}_p$, for which*

$$f(X) = \left(\prod_{i=1}^{m}(X-\alpha_i)\right) g(X)$$

Proof. Clear from the proof of the theorem. □

Corollary 3.3. *Let $f(X) = \sum a_n x^n$ be a non-zero power series which converges on $p^m\mathbb{Z}_p$, for some $m \in \mathbb{Z}$. Then $f(X)$ has a finite number of roots in $p^m\mathbb{Z}_p$.*

Proof. Define

$$g(X) = f(p^m X) = \sum a_n p^{mn} X^n,$$

Since $f(x)$ converges for $x \in p^m\mathbb{Z}_p$, $g(x) = f(p^m x)$ converges for $x \in \mathbb{Z}_p$, applying the theorem to $g(X)$ gives the finiteness of its zeros. □

Corollary 3.4. *Let $f(X) = \sum a_n x^n$ and $g(X) = \sum b_n X^n$ be two p-adic power series which converge in a disc $p^m\mathbb{Z}_p$. If there exist infinitely many numbers $\alpha \in p^m Z_p$ such that $f(\alpha) = g(\alpha)$, then $a_n = b_n, \forall n \geq 0$*

Proof. Define

$$h(X) = f(X) - g(X) = \sum (a_n - b_n) X^n$$

, then $h(X)$ converges also on $p^m\mathbb{Z}_p$, by Corollary 3.3 $h(X)$ has to have finitely many zeros, otherwise it must be the zero power series. Which means that

$$f(X) = g(X) \implies a_n = b_n \forall n \geq 0$$

□

Corollary 3.5. *Let $f(X) = \sum a_n x^n$ be a p-adic power series which converges in some disc $p^m\mathbb{Z}_p$. If the function $p^m\mathbb{Z}_p \to \mathbb{Q}_p, x \mapsto f(x)$ is periodic, that is, $\exists \pi \in p^m\mathbb{Z}_p : f(x+\pi) = f(x), \forall \in p^m\mathbb{Z}_p$ then $f(X)$ is constant.*

Proof. The series $f(X) - f(0)$ has zeros at $n\pi$ for all $n \in \mathbb{Z}$, since $\pi \in p^m\mathbb{Z}_p$ implies $n\pi \in p^m\mathbb{Z}_p$, this gives infinitely many zeros, and hence the series $f(X) - f(0)$ must be identically zero, i.e. $f(X)$ must be constant. □

Corollary 3.6. *Let $f(X) = \sum a_n x^n$ be a p-adic power series which is entire, that is, $f(x)$ converges $\forall x \in \mathbb{Q}_p$. Then $f(X)$ has at most countably many zeros. Furthermore, if the set of zeros is not finite then the zeros form a sequence α_n with $|\alpha_n| \to \infty$.*

Proof. This is clear, because the number of zeros in each bounded disk $p^m\mathbb{Z}_p$ is finite. □

4 The p-adic Logarithm Function

Definition 4.1 (Formal power series for the logarithm)**.**

$$\mathbf{log}(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} \mp \cdots \in \mathbb{Q}_p[[X]]$$

Since the coefficients are in $\mathbb{Q}$ we can consider it as a power series with coefficients in $\mathbb{Q}_p$

Remark 4.2. We use **log** when referring to the formal power series, not the logarithm function itself.

Proposition 4.3. $\mathbf{log}(1+X)$ *converges if and only if* $|x| < 1 \iff x \in p\mathbb{Z}_p$

Proof. $\mathbf{log}(1+X)$ is given by the power series

$$\mathbf{log}(1+X) = f(X) = \sum_{n \geq 1} a_n X^n = \sum_{n \geq 1} (-1)^{n+1} \frac{X^n}{n}, \quad a_n = \frac{(-1)^{n+1}}{n}$$

So by Proposition 1.3 the radius of convergence is

$$\rho = \left(\limsup_{n\to\infty} \sqrt[n]{|a_n|} \right)^{-1} = \left(\limsup_{n\to\infty} \sqrt[n]{\left| \frac{(-1)^{n+1}}{n} \right|} \right)^{-1} = \left(\limsup_{n\to\infty} \sqrt[n]{\left| \frac{1}{n} \right|} \right)^{-1} = \left(\limsup_{n\to\infty} \sqrt[n]{p^{-v_p(1/n)}} \right)^{-1}$$

$$= \left(\limsup_{n\to\infty} \sqrt[n]{p^{v_p(n) - v_p(1)}} \right)^{-1} = \left(\limsup_{n\to\infty} p^{v_p(n)/n} \right)^{-1}$$

we have

$$\frac{v_p(n)}{n} \leq \frac{\log(n)}{\log(p)n} \xrightarrow{n\to\infty} 0 \implies \rho = 1$$

This doesn't tell us the entire story however, we have to determine if $\mathbf{log}(1+X)$ converges for $|x| \leq \rho$ or for $|x| < \rho$, so we check if $\lim_{n\to\infty} |a_n|\rho^n$, by Prop. 2.1 - Talk 8, we have

$$\lim_{n\to\infty} |a_n|\rho^n = \lim_{n\to\infty} |a_n| = \lim_{n\to\infty} p^{v_p(n)} \neq 0$$

Since $v_p(n) = 0$ whenever n doesn't divide p. □

Definition 4.4. Let $U_1 = B(1,1) = \{x \in \mathbb{Z}_p : |x-1| < 1\} = 1 + p\mathbb{Z}_p$, we define the p-adic logarithm of $x \in U_1$ as:

$$\log_p(x) = \mathbf{log}(1 + (x-1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$$

In order to be able to call it a logarithm, it has to fill the usual logarithmic property:

Proposition 4.5. *Let $a, b \in 1 + p\mathbb{Z}_p$, then we have*

$$\log_p(ab) = \log_p(a) + \log_p(b)$$

Proof. Let $x, y \in p\mathbb{Z}_p$ such that $a = 1 + x, b = 1 + y$, and define for $x \in p\mathbb{Z}_p$

$$f(x) = \log_p(1 + x) = \sum_{n\geq 1}(-1)^{n+1}\frac{x^n}{n}$$

$$f'(x) = \sum_{n\geq 1}(-1)^{n+1}x^{n-1} = \sum_{n\geq 0}(-1)^n x^n = \sum_{n\geq 0}(-x)^n = \frac{1}{1+x}$$

$$g(x) = \log_p((1 + x)(1 + y)) = \log_p(1 + y + (1 + y)x) = f(y + (1 + y)x)$$

By 165, $g(x)$ converges $\iff$ $f(x)$ converges $\iff$ $|x| < 1$, now we use the Chain Rule from Theorem 2.1 to compute the derivative of g:

$$g'(x) = (1 + y)f'(y + (1 + y)x) = \frac{1+y}{1+y+(1+y)x} = \frac{1}{1+x} = f'(x)$$

Since both $f(x), g(x)$ are defined by power series that converge for $|x| < 1$, by Corollary 2.5 it follows that $g(x) = f(x) + c$, for $|x| < 1$, to find c, we plug $x = 0$ and see that

$$c = g(0) = \log_p((1 + 0)(1 + y)) = \log_p(1 + y) = f(y)$$

$$\implies g(x) = f(x)+f(y) \implies \log_p((1+x)(1+y)) = \log_p(1+x)+\log_p(1+y) \iff \log_p(ab) = \log_p(a)+\log_p(b).$$

□

5 Roots of Unity in $\mathbb{Q}_p$

Proposition 5.1. *For $p \neq 2$ we have $\log_p(x) = 0 \iff x = 1$ and for $p = 2$, we have $\log_p(x) = 0 \iff x = \pm 1$.*

Proof. We know that $\log_p(x)$ converges only for $x \in p\mathbb{Z}_p$, not in $\mathbb{Z}_p$, but we can do a change of variables like in Corollary 3.3, so define $f(X) = \mathbf{log}(1 + px)$, this converges now for all $x \in \mathbb{Z}_p$ and we have

$$f(X) = \sum_{n\geq 1}(-1)^{n+1}\frac{p^n X^n}{n} = \sum_{n\geq 1} a_n X^n, \quad a_n = (-1)^{n+1}\frac{p^n}{n}$$

Now we have to look for the N like in Strassman's Theorem.

$$|a_n| = \left|(-1)^{n+1}\frac{p^n}{n}\right| = \left|\frac{p^n}{n}\right| = p^{-v_p(p^n/n)} = p^{v_p(n)-v_p(p^n)} = p^{v_p(n)-n}$$

Now by the definition of v_p, we can say that

$$v_p(n) = \lfloor \log_p(n)\rfloor \approx \log_p(n)$$

So we can approximate $p^{v_p(n)-n}$ as

$$p^{v_p(n)-n} \approx p^{\log_p(n)-n} = np^{-n} =: g(n)$$

And now we just have a problem in real analysis, and we need to find the maxima of g, so consider

$$g'(x) = p^{-x}(1 - x\log(p)) = 0 \iff x\log(p) = 1 \iff x = \frac{1}{\log(p)}$$

Now we know that $\log(p) < 1 \iff p < e, \log(p) > 1 \iff p > e$, since 2 is the only prime which is less than e, we have

$$x = \frac{1}{\log(p)} > 1 \iff p < e \iff p = 2$$

And otherwise

$$x < 1 \iff p > e \iff p \neq 2$$

So we know for sure, that the maximum index is 1 for $p \neq 2$, and 2 for $p = 2$, applying Strassman's Theorem, we get that $\log_p$ has 2 zeros in $\mathbb{Z}_2$, and 1 in $\mathbb{Z}_{p\neq 2}$, we can confirm this by checking

$$\log_p(1 + (1 - 1)) = \sum_{n\geq 1}(-1)^{n+1}(1 - 1)^n/n = 0$$

And for $p = 2$, we have to check if -1 is in $B(1, 1)$,

$$| - 1 - 1|_2 = | - 2|_2 = p^{-v_2(-2)} = 1/2 < 1 \implies -1 \in B(1, 1)$$

$$\log_p(1) = \log_p((-1)^2) = 2\log_p(-1) = 0.$$

□

Proposition 5.2. *Let $p \neq 2, x \in \mathbb{Q}_p$ and $x^p = 1$, then $x = 1$.*

Proof.

$$x^p = 1 \implies x \in \mathbb{Z}_p \implies \bar{x}^p = 1 \text{ in } \mathbb{Z}_p/p\mathbb{Z}_p$$
$$\implies \bar{x}^p = 1 \text{ in } \mathbb{Z}/p\mathbb{Z}$$

Now by Fermat's little theorem we know that

$$\bar{x}^{p-1} \equiv 1 \mod p \iff \bar{x}^p \equiv x \mod p.$$

and since $\bar{x}^p \equiv 1 \mod p$ we have $x \equiv 1 \mod p$, so $x \in 1 + p\mathbb{Z}_p$.

$$x \in 1 + p\mathbb{Z}_p, x^p = 1 \iff \log_p(x^p) = \log_p(1) \iff \log_p(x) = 0 \iff x = 1.$$

So there are no nontrivial p-th roots of unity in $\mathbb{Q}_p$, for $p \neq 2$. □

Proposition 5.3. *If $p = 2, x \in \mathbb{Q}_2$ and $x^4 = 1$ then $x = \pm 1$, which means that there are no fourth roots of unity in $\mathbb{Q}_2$*

Proof. Hence there are no p-th or p^n-th roots of unity in $\mathbb{Q}_p$, touching back to Talk 6, remark 4.5. □

Remark 5.4. We now summarize what we know so far about the roots of unity in $\mathbb{Q}_p$:

- If $p = 2$, then the only roots of unity are ± 1
- If $p \neq 2$, then $\mathbb{Q}_p$ contains all the $p-1$-st roots of unity and none other. (their existence was shown in Talk 6)

6 Miscellaneous

Remark 6.1. Let $(R, +, \cdot)$ be a ring, $x, y \in R$, then we have $x^n - y^n = (x - y)\sum_{j=0}^{n-1} x^j y^{n-1-j}, \forall n \in \mathbb{N}_0$

Proof. We do induction on n, Base case: $n = 2$, it's easy to see that

$$(x - y)\sum_{j=0}^{n-1} x^j y^{n-1-j} = (x - y)(x + y) = x^2 - y^2$$

Induction hypothesis: we assume for an arbitrary $n \geq 2 : x^n - y^n = (x - y)\sum_{j=0}^{n-1} x^j y^{n-1-j}$, Induction step: consider

$$(x - y)\sum_{j=0}^{n} x^j y^{n-j} = (x - y)(y^n + y^{n-1}x + \cdots + x^{n-1}y + x^n)$$

$$= (x - y)(y(y^{n-1} + y^{n-2}x + \cdots + yx^{n-2} + x^{n-1}) + x^n) = y\underbrace{(x - y)\sum_{j=0}^{n-1} x^j y^{n-1-j}}_{=x^n - y^n} + x^n(x - y)$$

$$= y(x^n - y^n) + x^n(x - y) = yx^n - y^{n+1} + x^{n+1} - yx^n = x^{n+1} - y^{n+1}.$$

□

Lemma 6.2. *Let $f(X) \in \mathbb{Q}_p[[X]]$ be a non-zero power series which converges $\forall x \in \mathbb{Z}_p$, then $\exists N \in \mathbb{N}_0$ such that $|a_N| = \max_{n \in \mathbb{N}_0} |a_n|$ and $|a_n| < |a_N|$ $\forall n > N$*

Proof. Since $f(X)$ converges $\forall x \in \mathbb{Z}_p$, then we have

$$\forall x \in \mathbb{Z}_p : \lim_{n \to \infty} |a_n x^n| = 0 = \lim_{n \to \infty} |a_n| \cdot |x^n| \implies \lim_{n \to \infty} |a_n| = 0$$

□

References

[Gou] Fernando Q. Gouvêa: *p-adic Numbers.*