Talk 9: Strassman's theorem and the Logarithm function

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 $|\sum a_n| \leq \max_n |a_n|$.*

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

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

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

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 $|x| < \rho$.*

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 $\rho' \geq \rho$.*

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 $f(X) = g(X) + c$.*

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 $f : \mathbb{Z}_p \to \mathbb{Q}_p, x \mapsto f(x)$ has at most N zeros.

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*

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

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 $p^m\mathbb{Z}_p$.*

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 $a_n = b_n, \forall n \geq 0$*

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.*

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.*

4 The p-adic Logarithm Function

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

$$\mathbf{log}(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1}\frac{X^n}{n} = X - \frac{X^2}{2} + \frac{X^3}{3} \mp \cdots$$

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* $|x| < 1 \iff x \in p\mathbb{Z}_p$

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*

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

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 $\log_p(x) = 0 \iff x = \pm 1$.*

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

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 $\mathbb{Q}_2$*

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)

References

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