Talk 9: Strassman's theorem and the Logarithm function

1 Revision

Remark 1.1. [Gou, Prop. 5.4.1] Let $f(X) \in \mathbb{Q}_p[[X]]$ be a power series, then the radius of convergence is $\rho = \frac{1}{(\limsup_{n\to\infty} \sqrt[n]{|a_n|})}$

Proposition 1.2. *[Gou, Prop. 5.1.4] Let $b_{ij} \in \mathbb{Q}_p$ and suppose $\forall i : \lim_{j\to\infty} b_{ij} = 0$ and $\lim_{i\to\infty} b_{ij} = 0$ uniformly in j, then both series $\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)$ and $\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$ converge and have equal sum.*

2 Strassman's Theorem

Remark 2.1. Let $(R, +, \cdot)$ be a ring, $x, y \in R$, then we have $x^n - y^n = (x - y)\sum_{j=0}^{n-1} x^j y^{n-1-j}, \forall n \in \mathbb{N}_0$

Lemma 2.2. *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 $|a_n| < |a_N|\ \forall n > N$*

Theorem 2.3 (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 $N \in \mathbb{N}_0$ like in Lemma 2.2 then the function f has at most N zeros.*

Corollary 2.4. *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 2.5. *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 2.6. *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 2.7. *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 2.8. *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 $|\alpha_n| \to \infty$.*

3 Formal Derivatives

Theorem-Definition 3.1. *Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$, we define its **formal derivative** as*

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

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 3.2. *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 $|x| < \rho$.*

4 The p-adic Logarithm Function

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

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

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* $|x| < 1$

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

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 $x = 1$.*

Corollary 5.3. *(Remark 4.5 in Talk 6) There are no p-th and hence no p^n-th roots of unity in $\mathbb{Q}_p$.*

Proposition 5.4. *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 5.5. 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.*