

# 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

$$\rho = \frac{1}{\limsup_{n \rightarrow \infty} \sqrt[n]{|a_n|}}$$

**Proposition 1.2.** [Gou, Prop. 5.1.4][Proposition 1.5 in Talk 8] Let  $b_{ij} \in \mathbb{Q}_p$  and suppose  $\forall i : \lim_{j \rightarrow \infty} b_{ij} = 0$  and  $\lim_{i \rightarrow \infty} b_{ij} = 0$  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  $x^n - y^n = (x - y) \sum_{j=0}^{n-1} x^j y^{n-1-j}$ ,  $\forall n \in \mathbb{N}_0$

*Proof.* , we use 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

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

□

**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  $|a_n| < |a_N| \forall n > N$

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

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

□

**Theorem 2.3** (Strassman). Let  $f(X) \in \mathbb{Q}_p[[X]]$  and suppose we have  $\lim_{n \rightarrow \infty} a_n = 0$ , 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.

*Proof.* induction on  $N$ .

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

$$\begin{aligned} 0 &= f(x) = a_0 + a_1x + a_2x^2 + \cdots \\ \implies |a_0| &= |a_1x + a_2x^2 + \cdots| \leq \max_{n \geq 1} |a_n x^n| \leq \max_{n \geq 1} |a_n| \end{aligned}$$

But this contradicts the assumption that  $|a_0| > |a_n|, \forall n \geq 1$ , 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  $x \in \mathbb{Z}_p$

$$\begin{aligned} f(x) &= f(x) - f(\alpha) = \sum_{n=0}^{\infty} a_n x^n - \sum_{n=0}^{\infty} a_n \alpha^n = \sum_{n=0}^{\infty} a_n (x^n - \alpha^n) \stackrel{2.1}{=} (x - \alpha) \sum_{n=0}^{\infty} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j} \\ &= (x - \alpha) \sum_{n=0}^{\infty} \sum_{j=0}^{\infty} c_{nj}, \quad c_{nj} := \begin{cases} a_n x^j \alpha^{n-1-j} & j < n, \\ 0 & j \geq n. \end{cases} \end{aligned}$$

We can use prop 1.1 to change the order of the summation but first we have to show the conditions of the proposition:

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

$$\begin{aligned} &= (x - \alpha) \sum_{j=0}^{\infty} \sum_{n=j+1}^{\infty} a_n x^j \alpha^{n-1-j} = (x - \alpha) \sum_{j=0}^{\infty} x^j \underbrace{\sum_{n=0}^{\infty} a_{n+j+1} \alpha^n}_{=: b_j} \\ &= (x - \alpha) g(x), \quad g(x) := \sum_{j=0}^{\infty} b_j x^j \end{aligned}$$

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  $b_j \rightarrow 0$

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

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

$$|b_{N-1}| = |a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \dots| = |a_N|$$

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

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

So the index at which the maximum coefficient is reached  $b_n$  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  $\alpha$ ).

□

**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  $\alpha_1, \dots, \alpha_m \in \mathbb{Z}_p$  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 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  $p^m \mathbb{Z}_p$ .

*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 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  $\alpha \in p^m \mathbb{Z}_p$  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 2.5  $h(X)$  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 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  $p^m \mathbb{Z}_p \rightarrow \mathbb{Q}_p, x \mapsto f(x)$  is periodic, that is,  $\exists \pi \in p^m \mathbb{Z}_p : f(x + \pi) = f(x), \forall x \in p^m \mathbb{Z}_p$  then  $f(X)$  is constant.

*Proof.* □

**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  $\alpha_n$  with  $|\alpha_n| \rightarrow \infty$ .

### 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:*  $(f \circ g)'(X) = f'(g(X))g'(X)$

*Proof.* □

**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).

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

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.**  $\log(1 + X)$  converges if and only if  $|x| < 1$

*Proof.* □

**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:

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

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  $x \in p\mathbb{Z}_p$

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

□

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

*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 2.5  $\square$

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

*Proof.*  $\square$

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

*Proof.*  $\square$

**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  $\mathbb{Q}_2$*

*Proof.*  $\square$

**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  $\pm 1$
- 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*.