

## SOLUTION TO EXERCISE 5.3

ADRIAN BRUNYATE AND ALEX RICE

Let  $K$  be a finite extension of  $\mathbb{Q}_p$  with ramification index  $e$ . Let  $v$  be the usual integer-valued discrete valuation on  $K$ ,  $R = \{x \in K | v(x) \geq 0\}$  the valuation ring, and  $\mathfrak{m} = \{x \in K | v(x) > 0\}$  the unique maximal ideal.

Let  $\mathcal{U}^n = 1 + \mathfrak{m}^n$ . As  $\mathcal{U}^n$  is the kernel of the map on unit groups induced by the quotient  $R \rightarrow R/\mathfrak{m}^n$ , it is, in particular, a multiplicative group.

**Claim.** *For  $n \geq \max\{\frac{2e}{p-1}, e \log_p 2\}$ , there is a canonical isomorphism of groups  $L : (\mathcal{U}^n, \cdot) \rightarrow (\mathfrak{m}^n, +)$ .*

*Proof.* We will give this isomorphism and its inverse explicitly, via “logarithmic” and “exponential” maps, which we first introduce below as formal power series.

$$L(t) := \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(t-1)^k}{k}, \quad E(t) := \sum_{k=0}^{\infty} \frac{t^k}{k!} \in \mathbb{Q}[[t]].$$

We recognize  $L$  as the usual Taylor expansion for  $\log t$  around  $t = 1$ , and  $E$  as the expansion of  $e^t$  around  $t = 0$ . As functions on  $\mathbb{C}$ ,  $L$  and  $E$  are inverses on small discs around 1 and 0, respectively, so in particular, we must have the equality  $L(E(t)) = E(L(t)) = t$  as formal power series with  $\mathbb{Q}$ -coefficients (and hence also as formal power series with coefficients in any field of characteristic 0). Similarly, we have the formal identities required to eventually assert that  $L$  and  $E$  define appropriate group homomorphisms, namely  $L(xy) = L(x) + L(y)$  and  $E(x+y) = E(x)E(y)$ . With these facts in mind, it will suffice to show the following for  $n \geq \max\{\frac{2e}{p-1}, e \log_p 2\}$ :

- i) If  $x \in \mathcal{U}^n$ , then  $L(x)$  converges as an infinite sum in  $K$ , hence defining a homomorphism  $L : (\mathcal{U}^n, \cdot) \rightarrow (K, +)$ .
- ii)  $L(\mathcal{U}^n) \subset \mathfrak{m}^n$ .
- iii) If  $x \in \mathfrak{m}^n$ , then  $E(x)$  converges as an infinite sum in  $K$ , which therefore, assuming all values are nonzero, defines a homomorphism  $E : (\mathfrak{m}^n, +) \rightarrow (K^\times, \cdot)$ .
- iv)  $E(\mathfrak{m}^n) \subset \mathcal{U}^n$ .

For i), we see that if  $x \in \mathcal{U}^n$ , then  $v((x-1)^k) \geq nk$ , whereas  $v(k) \leq e \log_p k$ . Therefore  $v(\frac{(x-1)^k}{k}) \rightarrow \infty$ , so  $\frac{(x-1)^k}{k} \rightarrow 0$ , and hence  $L(x)$  converges.

For ii), however, we need that  $v(\frac{(x-1)^k}{k}) \geq n$  for ALL  $k$ , for which it would suffice to have  $nk - e \log_p k \geq n$  for all  $k$ . One can check that this inequality is guaranteed

for all  $k$  if we merely insist it for  $k = 2$ , yielding  $n \geq e \log_p 2$ .

For iii), we see that if  $x \in \mathfrak{m}^n$ , then  $v(x^k) \geq nk$ , whereas

$$v(k!) \leq v(p)\left(\frac{k}{p} + \frac{k}{p^2} + \dots\right) = ek\left(\frac{\frac{1}{p}}{1 - \frac{1}{p}}\right) = \frac{ek}{p-1} \leq \frac{nk}{2},$$

provided  $n \geq \frac{2e}{p-1}$ . Therefore,  $v\left(\frac{x^k}{k!}\right) \rightarrow \infty$ , so  $\frac{x^k}{k!} \rightarrow 0$ , hence  $E(x)$  converges.

For iv), we need that

$$v\left(\frac{x^k}{k!}\right) \geq nk - \frac{ek}{p-1} \geq n \text{ for all } x \in \mathfrak{m}^n, k \geq 1,$$

which again holds provided  $n \geq \frac{2e}{p-1}$ .

□

Note that in the special case of a totally unramified extension, in particular  $\mathbb{Q}_p$  itself, this isomorphism is valid for all  $n \in \mathbb{N}$  when  $p \geq 3$ , and for  $n \geq 2$  for  $p = 2$ .

Remark [PLC]: This result is as false as it gets for local fields of positive characteristic (c.f. Exercise 5.4): there is no nontrivial group homomorphism from the unit group  $\mathbb{F}_q[[t]]^\times$  to the additive group  $\mathbb{F}_q[[t]]$ , since the former has no elements of order  $p$  and the latter is a  $p$ -torsion group. This may be viewed as an analytic indication of the fact that the additive group and the multiplicative group are distinct **formal groups** in positive characteristic, which has implications in the theory of abelian varieties. Also note that the proof does not have a chance to get started because the formal power series which define the logarithm and the exponential are not well-defined in positive characteristic. Nevertheless, one sometimes encounters the **Artin-Hasse exponential**  $\sum_{n=0}^{p-1} \frac{t^n}{n!}$  when doing arithmetic geometry in positive characteristic...