

Elliptic Curves. MT 2025. Sheet 3.

Section A

1. Let K be a field, complete with respect to a non-Archimedean valuation $|\cdot|$, and let $R = \{x \in K : |x| \leq 1\}$. Let $f(X) \in R[x]$ be a monic polynomial with discriminant D , and let $a_0 \in R$ satisfy $|f(a_0)| < |D|^2$. Show that $f(X)$ has a root $a \in R$.
(Hint: use Comment 1.17(a) in lecture notes.)
2. Let $\mathcal{E} : Y^2 = X^3 + 17$, defined over $\mathbb{Q}$, and $\tilde{\mathcal{E}} : Y^2 = X^3 + 2$, defined over $\mathbb{F}_5$. What does $(-64/25, 59/125) \in \mathcal{E}(\mathbb{Q})$ map to under the reduction map modulo 5?

Section B

3. Show that the curve $2Y^2 = X^4 - 17$ has points in $\mathbb{R}$ and every $\mathbb{Q}_p$, but not in $\mathbb{Q}$.
(Hint: For showing that there are points in every $\mathbb{Q}_p$, it is helpful to use Theorem 2.16. Note also that the curve is birationally equivalent to $V^2 = 2X^4 - 34$, where $V = 2Y$. For showing there are no points in $\mathbb{Q}$, first show that, if there were points in $\mathbb{Q}$, then there would exist $r, s, t \in \mathbb{Z}$ with $\gcd(r, t) = 1$ such that $2s^2 = t^4 - 17r^4$, and then show that any prime dividing s is a quadratic residue modulo 17.)
4. Give examples of elliptic curves defined over $\mathbb{Z}_p$ ($p \neq 2$) such that $\tilde{\mathcal{E}}$, defined over $\mathbb{F}_p$, has:
 - (a) A cusp which lifts to a point in $\mathcal{E}(\mathbb{Q}_p)$.
 - (b) A cusp which does not lift to a point in $\mathcal{E}(\mathbb{Q}_p)$.
 - (c) A node which lifts to a point in $\mathcal{E}(\mathbb{Q}_p)$.
 - (d) A node which does not lift to a point in $\mathcal{E}(\mathbb{Q}_p)$.
5. Let m be a positive integer and $F(X, Y) \in R[[X, Y]]$ a formal group. Prove that the multiplication by m series $[m](T) \in R[[T]]$ is a homomorphism from F to F .
6. Let K be a field, complete with respect to a discrete non-Archimedean valuation, with valuation ring R and maximal ideal $\mathfrak{m} = (\varpi)$ with uniformizer ϖ . Suppose the residue field $k = R/\mathfrak{m}$ has characteristic p and K has characteristic 0. Let F be a formal group defined over R .
(You might find it helpful to use the result in Question 10 below.)
 - (a) Show that the power series $\log_F$ defines a homomorphism

$$(F(\mathfrak{m}), \oplus) \rightarrow (K, +)$$
 - (b) Suppose $r \geq 1$ is an integer such that $|\varpi|^r < |p|^{1/(p-1)}$. Show that for $x \in \mathfrak{m}^r$, $|\log_F(x)| = |x|$, and deduce that the restriction of $\log_F$ to $(F(\mathfrak{m}^r))$ is injective.
 - (c) Use part (b) to give an alternative proof of the $n = 1$ case of Theorem 5.19 in the lecture notes.

7. Find the torsion group over $\mathbb{Q}$ for each of:

(a) $Y^2 = X^3 + 1$. (b) $Y^2 = X(X-1)(X-2)$. (c) $Y^2 = X^3 + 1/3^6$.

Section C

8. A *non-commutative formal group* over a ring R is a power series $F(X, Y) \in R[[X, Y]]$ which satisfies:

- $F(X, Y) = X + Y + \text{terms of degree } \geq 2$,
- $F(X, F(Y, Z)) = F(F(X, Y), Z)$ [associativity],
- but *not* $F(X, Y) = F(Y, X)$ [commutativity].

Let $R = \mathbb{F}_p[t]/I$, where $I = t^2\mathbb{F}_p[t]$. Find a non-commutative formal group over R .

(Hint: you may find it helpful to consider formal group laws of the form $F(X, Y) = X + Y + tG(X, Y)$, where $G(X, Y) \in R[[X, Y]]$.)

9. Let $\mathcal{E} : Y^2 = X^3 + AX$, where $A \in \mathbb{Z}$ and $A \neq 0$. Let $F(X, Y)$ be the formal group associated to $\mathcal{E}$ [as in lectures] and let $F(X, Y) = \sum F_n(X, Y)$, where each $F_n(X, Y)$ is homogeneous of degree n . Show that $F_n(X, Y) = 0$ unless $n \equiv 1 \pmod{4}$.

What is the similar result when the elliptic curve is of the form $\mathcal{E} : Y^2 = X^3 + B$?

10. The following result is useful for checking that composition of formal power series interacts well with composing the associated functions.

Let K be a field, complete with respect to a non-Archimedean valuation, with valuation ring R and maximal ideal $\mathfrak{m}$. Suppose we have a power series

$$F(X_1, \dots, X_k) = \sum_{n=(n_i)_{i=1}^k} a_n X_1^{n_1} \dots X_k^{n_k} \in K[[X_1, \dots, X_k]]$$

and a k -tuple of power series

$$G_i(X_1, \dots, X_l) \in R[[X_1, \dots, X_l]] : 1 \leq i \leq k$$

with no constant term.

Consider the composed formal power series

$$(F \circ G)(X_1, \dots, X_l) := F(G_1(X_1, \dots, X_l), \dots, G_k(X_1, \dots, X_l)) \in K[[X_1, \dots, X_l]].$$

Suppose that for each positive real number $\rho < 1$, the set

$$\{|a_n| \rho^{\sum n_i} : n \in \mathbb{Z}_{\geq 0}^k\}$$

is bounded. Prove that for all $(x_i) \in \mathfrak{m}^l$ we have

$$(F \circ G)(x_1, \dots, x_l) = F(G_1(x_1, \dots, x_l), \dots, G_k(x_1, \dots, x_l)).$$

(This includes the claim that the two sides of the equation converge!)

(You might think that the statement is automatic as long as everything converges, but this isn't the case. See Problem 148 and pg. 120 in Gouvêa's book 'p-adic numbers' for examples illustrating this.)