Chapter III. $p$-Adic Addition

In this chapter we investigate addition on the elliptic curve in relation to divisibility properties of the denominators of its coordinates, and the quadraticity of the additional formula. This takes place in the general framework that a Lie group has an exponential map convergent near the origin, and giving one-parameter analytic subgroups. We want to see what happens when the base field is $p$-adic. As before, we carry out the theory ad hoc in a simple manner, making use of the addition formulas given explicitly on the elliptic curve, without fancy language.

The $p$-adic study of elliptic curves was originated by Lutz [Lu], see also Weil [We 3]. For the exponential map on abelian varieties or algebraic groups, cf. Mattuck [Mat], Igusa [Ig], and Serre’s notes [Se 3]. Cf. also the discussion by Tate in his general report [Ta 1]. The exposition of this chapter also owes much to other notes of Tate, from his Phillips Lectures at Haverford College, and to his article [Ta 2]. For simplicity we usually limit ourselves to curves defined by an equation

$$y^2 = x^3 + ax + b,$$

instead of the general equation also valid in characteristic 2 and 3, for which normal forms were originally given by Deuring. By referring to [Ta 1] and [Ta 2], the reader can work such cases out for himself.

Throughout this chapter, we let $R$ be an integral domain with quotient field $K$, and assume that $R$ is a principal ideal ring. The reader may assume that $R$ has characteristic 0, but what we say will be true in characteristic $\neq 2, 3$, and, suitably formulated is even true in all characteristics.

The ordinary integers constitute an example of such a ring. If $p$ is a prime number, the local ring $\mathbb{Z}_{(p)}$, consisting of all quotients $m/n$, where $(n, p) = 1$ has a unique prime element $p$, and unique factorization in this ring is of the form

$$a = p^ru$$

where $u$ is a unit in $\mathbb{Z}_{(p)}$, i.e. the numerator and denominator of $u$ are not divisible by $p$. More generally, if $\pi$ is a prime element of $R$, then one may similarly form the local ring $R_{(\pi)}$, consisting of all elements $a/b$, with $a, b \in R$ and $b$ not divisible by $\pi$. Unique
factorization in \( R_{(\pi)} \) is of the form

\[ a = \pi^r u, \]

where \( u \) is a unit in \( R_{(\pi)} \). We call \( r = \text{ord}_n a \).

Sections § 4, § 5 and § 6 may be omitted without impairing the logical development of the theory of the height, and of the rest of the book, save for the more refined results.

§ 1. Addition Near the Origin

For this entire section, we assume in addition that \( R \) has a single prime element (up to units), which we denote by \( \pi \). Then \( R \) has a unique maximal ideal \( (\pi) = R\pi \).

We suppose as before that \( A \) is defined by the equation

\[ y^2 = x^3 + ax + b \]

and assume that \( a, b \in R \).

If \( x = \pi^{-r} u \) where \( u \) is a unit in \( R \), and \( r \geq 0 \), then we say that \( x \) has a pole of order \( r \) (at \( \pi \)). Suppose \((x, y)\) is a point on \( A \) with coordinates \( x, y \in K \), and \( x \) has a pole of order \( \geq 1 \). Then \( x^3 + ax + b \) has a pole of order 3 times the order of the pole of \( x \), and consequently \( y \) must also have a pole. It then follows that there exist units \( u, u' \) in \( R \) such that

\[ x = \frac{u}{\pi^{2r}} \quad \text{and} \quad y = \frac{u'}{\pi^{3r}} \]

for some integer \( r \geq 1 \). Thus \( x \) has a pole of even order, and \( y \) has a pole of order divisible by 3.

For \( r > 0 \) we let \( A(\pi^r) \) be the set of points \( P \) in \( A(K) \) such that \( P \) is at infinity, or the denominator of \( x(P) \) is divisible by \( \pi^{2r} \). In this case, this denominator is of the form \( \pi^{2r} \), and the denominator of \( y(P) \) is of the form \( \pi^{3r} \).

We let

\[ t = x/y \quad \text{and} \quad s = 1/y . \]

In terms of the coordinates \( t, s \) the equation for the curve becomes

\[ s = t^3 + as^2 t + bs^3 . \]

Viewing the curve as embedded in projective plane, the new coordinates are such that the point at infinity in terms of the \((x, y)\) coordinates is transformed to the point \((0, 0)\) in terms of the \((t, s)\) coordinates. One usually calls \( t \) a local parameter at the