Chapter 6

The p-adic Case

6.1 The p-adic valuation on $\mathbb{Q}$

The absolute value $|x|$ on $\mathbb{Q}$ defines the metric, or distance function,

$$d(x, y) = |x - y|.$$

Surprisingly perhaps, there are other metrics on $\mathbb{Q}$ just as worthy of study.

Definition 6.1 *Let p be a prime. Suppose*

$$x = \frac{m}{n} \in \mathbb{Q},$$

where $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. Then we set

$$\|x\|_p = \begin{cases} 0 & \text{if } x = 0, \\ p^{-e} & \text{if } p^e \parallel m, \\ p^e & \text{if } p^e \parallel n. \end{cases}$$

We call the function $x \mapsto \|x\|_p$ the p-adic valuation *on $\mathbb{Q}$.*

Another way of putting this is: If $x \in \mathbb{Q}$, $x \neq 0$, then we can write

$$x = \frac{m}{n} p^e$$

where $p \nmid m, n$. The p-adic value of x is given by

$$\|x\|_p = p^{-e}.$$

Note that all integers are quite small in the p-adic valuation:

$$x \in \mathbb{Z} \Longrightarrow \|x\|_p \leq 1.$$

High powers of p are very small:

$$p^n \to 0 \text{ as } n \to \infty.$$

The following result is immediate.

Proposition 6.1 *1.* $\|x\|_p \geq 0$*; and* $\|x\|_p = 0 \iff x = 0$*;*

2. $\|xy\|_p = \|x\|_p \|y\|_p$*;*

3. $\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p)$.

From (3) we at once deduce

Corollary 1 *The p-adic valuation satisfies the triangle inequality:*

3' $\|x + y\|_p \leq \|x\|_p + \|y\|_p$.

A *valuation* on a field k is a map

$$x \mapsto \|x\| : k \to \mathbb{R}$$

satisfying (1), (2) and (3'). A valuation defines a *metric*

$$d(x, y) = \|x - y\|$$

on k; and this in turn defines a *topology* on k.

Corollary 2 *If* $\|x\|_p \neq \|y\|_p$ *then*

$$\|x + y\|_p = \max(\|x\|_p, \|y\|_p).$$

Corollary 3 *In a p-adic equation*

$$x_1 + \cdots + x_n = 0 \qquad (x_1, \ldots, x_n \in \mathbb{Q}_p)$$

no term can dominate, ie at least two of the x_i must attain $\max \|x_i\|_p$.

To emphasize the analogy between the p-adic valuation and the familiar valuation $|x|$ we sometimes write

$$\|x\|_\infty = |x|.$$

6.2 p-adic numbers

The reals $\mathbb{R}$ can be constructed from the rationals $\mathbb{Q}$ by *completing* the latter with respect to the valuation $|x|$. In this construction each Cauchy sequence

$$\{x_i \in \mathbb{Q} : |x_i - x_j| \to 0 \text{ as } i, j \to \infty\}$$

defines a real number, with 2 sequences defining the same number if $|x_i - y_i| \to 0$.

(There are 2 very different ways of constructing $\mathbb{R}$ from $\mathbb{Q}$: by completing $\mathbb{Q}$, as above; or alternatively, by the use of *Dedekind sections*. In this each real number corresponds to a partition of $\mathbb{Q}$ into 2 subsets L, R where

$$l \in L,\ r \in R \Longrightarrow l < r.$$

The construction by completion is much more general, since it applies to any metric space; while the alternative construction uses the fact that $\mathbb{Q}$ is an *ordered* field. John Conway, in *On Numbers and Games,* has generalized Dedekind sections to give an extraordinary construction of rationals, reals and infinite and infinitesimal numbers, starting 'from nothing'. Knuth has given a popular account of Conway numbers in *Surreal Numbers.*)

We can complete $\mathbb{Q}$ with respect to the p-adic valuation in just the same way. The resulting field is called *the field of p-adic numbers*, and is denoted by $\mathbb{Q}_p$. We can identify $x \in \mathbb{Q}$ with the Cauchy sequence $(x, x, x, \dots)$. Thus

$$\mathbb{Q} \subset \mathbb{Q}_p.$$

To bring out the parallel with the reals, we sometimes write

$$\mathbb{R} = \mathbb{Q}_\infty.$$

The numbers $x \in \mathbb{Q}_p$ with $\|x\|_p \le 1$ are called *p-adic integers*. The p-adic integers form a ring, denoted by $\mathbb{Z}_p$. For if $x, y \in \mathbb{Z}_p$ then by property (3) above,

$$\|x + y\|_p \le \max(\|x\|_p, \|y\|_p) \le 1,$$

and so $x + y \in \mathbb{Z}_p$. Similarly, by property (1),

$$\|xy\|_p = \|x\|_p \|y\|_p \le 1,$$

and so $xy \in \mathbb{Z}_p$.

Evidently

$$\mathbb{Z} \subset \mathbb{Z}_p.$$

More generally,

$$x = \frac{m}{n} \in \mathbb{Z}_p$$

if $p \nmid n$. (We sometimes say that a rational number x of this form is *p-integral.*) In other words,

$$\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{m}{n} : p \nmid n\}.$$

Evidently the p-integral numbers form a sub-ring of $\mathbb{Q}$.

Concretely, each element $x \in \mathbb{Z}_p$ is uniquely expressible in the form

$$x = c_0 + c_1 p + c_2 p^2 + \cdots \quad (0 \le c_i < p).$$

More generally, each element $x \in \mathbb{Q}_p$ is uniquely expressible in the form

$$x = c_{-i} p^{-i} + c_{-i+1} p^{-i+1} + \cdots + c_0 + c_1 p + \cdots \quad (0 \le c_i < p).$$

We can think of this as the p-adic analogue of the decimal expansion of a real number $x \in \mathbb{R}$.

Suppose for example $p = 3$. Let us express $1/2 \in \mathbb{Q}_3$ in standard form. The first step is to determine if

$$\frac{1}{2} \equiv 0, 1 \text{ or } 2 \bmod 3.$$

In fact $2^2 \equiv 1 \bmod 3$; and so

$$\frac{1}{2} \equiv 2 \bmod 3.$$

Next

$$\frac{1}{3}\left(\frac{1}{2} - 2\right) = -\frac{1}{2} \equiv 1 \bmod 3$$

ie

$$\frac{1}{2} - 2 \equiv 1 \cdot 3 \bmod 3^2.$$

Thus

$$\frac{1}{2} \equiv 2 + 1 \cdot 3 \bmod 3^2$$

For the next step,

$$\frac{1}{3}\left(-\frac{1}{2} - 1\right) = -\frac{1}{2} \equiv 1 \bmod 3$$

giving

$$\frac{1}{2} \equiv 2 + 1 \cdot 3 + 1 \cdot 3^2 \bmod 3^3$$

It is clear that this pattern will be repeated indefinitely. Thus

$$\frac{1}{2} = 2 + 3 + 3^2 + 3^3 + \cdots .$$

To check this,

$$\begin{aligned}
2 + 3 + 3^2 + \cdots &= 1 + (1 + 3 + 3^2 + \cdots) \\
&= 1 + \frac{1}{1 - 3} \\
&= 1 - \frac{1}{2} \\
&= \frac{1}{2}.
\end{aligned}$$

As another illustration, let us expand $3/5 \in \mathbb{Q}_7$. We have

$$\begin{aligned}
\frac{3}{5} &\equiv 2 \bmod 7\\
\frac{1}{7}\left(\frac{3}{5}-2\right) &= -\frac{1}{5} \equiv 4 \bmod 7\\
\frac{1}{7}\left(-\frac{1}{5}-4\right) &= -\frac{3}{5} \equiv 5 \bmod 7\\
\frac{1}{7}\left(-\frac{3}{5}-5\right) &= -\frac{4}{5} \equiv 2 \bmod 7\\
\frac{1}{7}\left(-\frac{4}{5}-2\right) &= -\frac{2}{5} \equiv 1 \bmod 7\\
\frac{1}{7}\left(-\frac{2}{5}-1\right) &= -\frac{1}{5} \equiv 4 \bmod 7
\end{aligned}$$

We have entered a loop; and so (in $\mathbb{Q}_7$)

$$\frac{3}{5} = 2 + 4 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7^3 + 1 \cdot 7^4 + 4 \cdot 7^5 + 5 \cdot 7^6 + \cdots$$

Checking,

$$\begin{aligned}
1 + \left(1 + 4 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7\right)\frac{1}{1-7^4} &= 1 - \frac{960}{2400}\\
&= 1 - \frac{2}{5}\\
&= \frac{3}{5}.
\end{aligned}$$

It is not difficult to see that a number $x \in \mathbb{Q}_p$ has a recurring p-adic expansion if and only if it is rational (as is true of decimals).

Let $x \in \mathbb{Z}_p$. Suppose $\|x\|_p = 1$. Then

$$x = c + yp,$$

where $0 < c < p$ and $y \in \mathbb{Z}_p$. Suppose first that $c = 1$, ie

$$x = 1 + yp.$$

Then x is invertible in $\mathbb{Z}_p$, with

$$x^{-1} = 1 - yp + y^2p^2 - y^3p^3 + \cdots .$$

Even if $c \neq 1$ we can find d such that

$$dc \equiv 1 \bmod p.$$

Then

$$dx \equiv dc \equiv 1 \bmod p,$$

say

$$dx = 1 + py,$$

and so x is again invertible in $\mathbb{Z}_p$, with

$$x^{-1} = d\left(1 - yp + y^2p^2 - \cdots\right).$$

Thus the elements $x \in \mathbb{Z}_p$ with $\|x\|_p = 1$ are all *units* in $\mathbb{Z}_p$, ie they have inverses in $\mathbb{Z}_p$; and all such units are of this form. These units form the multiplicative group

$$\mathbb{Z}_p^{\times} = \{x \in \mathbb{Z}_p : \|x\|_p = 1\}.$$

6.3 In the p-adic neighbourhood of 0

Recall that an elliptic curve $\mathcal{E}(k)$ can be brought to Weierstrassian form

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6$$

if and only if it has a flex defined over k. This is not in general true for elliptic curves over $\mathbb{Q}_p$. For example, the curve

$$X^3 + pY^3 + p^2Z^3 = 0$$

has no points at all (let alone flexes) defined over $\mathbb{Q}_p$. For if $[X, Y, Z]$ were a point on this curve then

$$\|X^3\|_p = p^{3e},\ \|pY^3\|_p = p^{3f-1},\ \|p^2Z^3\|_p = p^{3g-2}$$

for some integers e, f, g. But if $a, b, c \in \mathbb{Q}_p$ and

$$a + b + c = 0$$

then two (at least) of a, b, c must have the same p-adic value, by Corollary 3 to Proposition F.1.

On the other hand, $\mathbb{Q}_p$ is of characteristic 0; so if $\mathcal{E}(\mathbb{Q}_p)$ *is* Weierstrassian — as we shall always assume, for reasons given earlier — then it can be brought to standard form

$$y^2 = x^3 + bx + c.$$

In spite of this, there is some advantage in working with the general Weierstrassian equation, since — as we shall see in Chapter 6 — this allows us to apply the results of this Chapter to study the integer points (that is, points with integer coordinates) on elliptic curves over $\mathbb{Q}$ given in general Weierstrassian form. Such an equation over $\mathbb{Q}$ can of course be reduced to standard form; but the reduction may well transform integer to non-integer points.

As in the real case, we study the curve in the neighbourhood of $0 = [0, 1, 0]$ by taking coordinates X, Z, where

$$(X, Z) = [X, 1, Z].$$

In these coordinates the elliptic curve takes the form

$$\mathcal{E}(\mathbb{Q}_p) : Z + c_1 XZ + c_3 Z^2 = X^3 + c_2 X^2 Z + c_4 XZ^2 + c_6 Z^3.$$

As in the real case, if $Z(P)$ is small then so is $X(P)$.

Proposition 6.2 *If $P \in \mathcal{E}(\mathbb{Q}_p)$ then*

$$\|Z\|_p < 1 \Longrightarrow \|X\|_p < 1;$$

and if this is so then

$$\|Z\|_p = \|X\|_p^3.$$

Proof ▶ Suppose $\|Z\|_p < 1$. Let

$$\|X\|_p = p^e.$$

If $e \geq 0$ then X^3 will dominate; no other term can be as large, p-adically speaking.

Thus $e < 0$, ie $\|X\|_p < 1$; and now each term

$$\|c_1 XZ\|_p, \|c_3 Z^2\|_p, \|c_2 X^2 Z\|_p, \|c_4 XZ^2\|_p, \|c_6 XZ\|_p < \|Z\|_p.$$

Only X^3 is left to balance Z. Hence

$$\|Z\|_p = \|X^3\|_p = \|X\|_p^3.$$

◀

Definition 6.2 *For each $e > 0$ we set*

$$\mathcal{E}_{(p^e)} = \{(X, Z) \in \mathcal{E} : \|X\|_p \leq p^{-e},\ \|Z\|_p \leq p^{-3e}\}.$$

Recall that in the real case, we showed that Z could be expressed as a power-series in X,

$$Z = X^3 - c_1 X^4 + (c_1^2 + c_2) X^5 + \cdots .$$

valid in a neighbourhood of $O = [0, 1, 0]$. It follows that

$$F(X, Z(X)) = 0$$

identically, where

$$F(X, Z) = Z + c_1 XZ + c_3 Z^2 - (X^3 + c_2 X^2 Z + c_4 XZ^2 + c_6 Z^3).$$

This identity must hold in any field, in particular in $\mathbb{Q}_p$.

Note that in the p-adic case, convergence is much simpler than in the real case. A series in $\mathbb{Q}_p$ converges if and only if its terms tend to 0:

$$\sum a_r \text{ convergent } \iff a_r \to 0.$$

Remember too that in the p-adic valuation integers are *small*,

$$x \in \mathbb{Z} \Longrightarrow \|x\|_p \leq 1.$$

Thus a power-series

$$a_0 + a_1 x + a_2 x^2 + \cdots$$

where $a_i \in \mathbb{Z}$—or more generally, $a_i \in \mathbb{Z}_p$—will converge for all x with $\|x\|_p < 1$.

Proposition 6.3 *Suppose $\|Z\|_p < 1$. Then we can express Z as a power-series in X,*

$$Z = X^3 + a_1 X^4 + a_2 X^5 + \cdots$$

where

1. $a_1 = -c_1,\ a_2 = c_1^2 + c_2,\ c_3 = -(c_1^3 + 2c_1 c_3 + c_3)$*;*
2. *each coefficient a_i is a polynomial in c_1, c_2, c_3, c_4, c_6 with integer coefficients;*
3. *the coefficient a_i has weight i, given that c_i is ascribed weight i for ($i = 1 - 4, 6$.*

Proof ▶ By repeatedly substituting for Z on the right-hand side of the equation

$$Z = X^3 + c_2 X^2 Z + c_4 X Z^2 + c_6 Z^3 - (c_1 X Z + c_3 Z^2)$$

we can successively determine more and more terms in the power series. Thus suppose we have shown that

$$Z = X^3 \left(1 + a_1 X + \cdots + a_{n-1} X^{n-1}\right).$$

On substituting for Z on the right-hand side of the equation and comparing coefficients of X^{n+3},

$$a_n = c_2 a_{n-2} + c_4 \sum_{i+j=n-4} a_i a_j + c_6 \sum_{i+j+k=n-6} a_i a_j a_k - c_1 a_{n-1} - c_3 \sum_{i+j=n-3} a_i a_j,$$

from which the result follows. ◀

Corollary *If the elliptic curve is given in standard form*

$$y^2 = x^3 + ax^2 + bx + c$$

then

$$Z = X^3 + d_2 X^5 + d_4 X^7 + \cdots,$$

where

1. *only odd powers of X appear, ie $d_i = 0$ for i odd;*
2. $d_2 = a,\ d_4 = a^2 + b,\ d_6 = a^3 + 3ab + c$;
3. *each coefficient d_{2i} is a polynomial in a, b, c with integer coefficients;*
4. *the coefficient d_{2i} has weight i, given that a, b, c are ascribed weights 2,4,6 respectively;*

Proof ▶ We note that in the standard case the (X, Z)-equation

$$Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

is invariant under the reflection $(X, Z) \mapsto (-X, -Z)$ (corresponding to $P \mapsto -P$). Thus

$$Z(-X) = -Z(X),$$

from which the absence of terms of even degree X^{2i} follows. ◀

As in the real case, the sum of 2 points near O is defined by a function $S(X_1, X_2)$, where

$$X(P_1 + P_2) = S(X(P_1), X(P_2)).$$

Proposition 6.4 *Suppose $\|X_1\|_p, \|X_2\|_p < 1$. Then we can express $S(X_1, X_2)$ as a double power-series in X_1, X_2,*

$$\begin{aligned} S(X_1, X_2) &= X_1 + X_2 + c_1 X_1 X_2 + \cdots \\ &= \sum_i S_i(X_1, X_2) \\ &= \sum_{i,j} s_{ij} X_1^i X_2^j \end{aligned}$$

where

1. *$S_i(X_1, X_2)$ is a symmetric polynomial in X_1, X_2 of degree i;*
2. $S_1(X_1, X_2) = X_1 + X_2,\ S_2(X_1, X_2) = c_1 X_1 X_2$;
3. *the coefficient s_{jk} of $X^j X^k$ is a polynomial in c_1, c_2, c_3, c_4, c_6 with integral coefficients.*
4. *all the coefficients in $S_i(X_1, X_2)$ have weight i.*

Proof ▶ As in the real case, let the line

$$P_1P_2 :\ Z = MX + D$$

meet $\mathcal{E}$ again in $P_3 = (X_3, Z_3)$, ie

$$P_3 = P_1 * P_2.$$

Then X_1, X_2, X_3 are the roots of the equation

$$\begin{aligned}X^3 + c_2X^2(MX+D) + c_4X(MX+D)^2 + c_6(MX+D)^3 \\ - (MX+D) - c_1X(MX+D) - c_3(MX+D)^2 = 0.\end{aligned}$$

Hence

$$\begin{aligned}X_1 + X_2 + X_3 &= -\frac{\text{coeff of } X^2}{\text{coeff of } X^3} \\ &= \frac{c_1M + 2c_3M^2 - (c_2 + c_4M + c_6M^2)D}{1 + c_2M + c_4M^2 + c_6M^3}\end{aligned}$$

Now

$$\begin{aligned}M &= \frac{Z_2 - Z_1}{X_2 - X_1} \\ &= \frac{X_2^3 - X_1^3}{X_2 - X_1} - c_1\frac{X_2^4 - X_1^4}{X_2 - X_1} + \cdots \\ &= X_1^2 + X_1X_2 + X_2^2 - c_1(X_1^3 + X_1^2X_2 + X_1X_2^2 + X_2^3) + \cdots, \\ D &= \frac{X_2Z_1 - X_1Z_2}{X_2 - X_1} \\ &= X_1X_2\left(\frac{X_2^2 - X_1^2}{X_2 - X_1} - c_1\frac{X_2^3 - X_1^3}{X_2 - X_1} + \cdots\right) \\ &= X_1X_2\left(X_1 + X_2 - c_1(X_2^2 + X_1X_2 + X_2^2) + \cdots\right).\end{aligned}$$

Thus M, D are both expressible as symmetric power-series in X_1, X_2; and

$$\|M\|_p \le p^{-2},\ \|D\|_p \le p^{-3},$$

or more precisely,

$$\begin{aligned}M &\equiv X_1^2 + X_1X_2 + X_2^2 \bmod p^3 \\ D &\equiv X_1X_2(X_1 + X_2) \bmod p^4.\end{aligned}$$

Hence

$$X_1 + X_2 + X_3 \equiv 0 \bmod p^2.$$

More precisely,

$$X_1 + X_2 + X_3 \equiv c_1(X_1^2 + X_1X_2 + X_2^2) \bmod p^3,$$

ie

$$X_3 \equiv -(X_1 + X_2) + c_1(X_1^2 + X_1X_2 + X_2^2) \bmod p^3.$$

In particular,

$$\|X_3\|_p \le p^{-1},$$

and so

$$\|Z_3\|_p = \|MX_3 + D\| \le p^{-3},$$

ie

$$P_1, P_2 \in \mathcal{E}_{(p)} \Longrightarrow P_3 \in \mathcal{E}_{(p)}.$$

Recall that

$$P_1 + P_2 = O * (P_1 * P_2) = O * P_3.$$

By our formulae above, with O, X_3 in place of X_1, X_2,

$$X(O * P_3) \equiv = -X_3 \bmod p^2,$$

or more precisely

$$X(O * P_3) \equiv = -X_3 + c_1 X_3^2 \bmod p^3,$$

Hence

$$X(P_1 + P_2) = X_1 + X_2 \bmod p^2,$$

or more precisely

$$\begin{aligned} X(P_1 + P_2) &= X_1 + X_2 - c_1(X_1^2 + X_1X_2 + X_2^2) + c_1(X_1 + X_2)^2 \bmod p^3 \\ &= X_1 + X_2 + c_1X_1X_2 \bmod p^3 \end{aligned}$$

◄

Finally, we turn to the normal coordinate function $\theta(X)$, defined as in the real case by

$$\begin{aligned} \frac{d\theta}{dX} &= \frac{1}{\partial F/\partial Z} \\ &= \frac{1}{1 + c_1X + 2c_3Z - c_2X^2 - 2c_4XZ - 3c_6Z^2} \end{aligned}$$

Proposition 6.5 *Suppose $\|X\|_p < 1$. Then we can express θ as a power-series in X,*

$$\begin{aligned} \theta = X + \frac{c}{2}X^2 + \cdots \\ = \sum t_n X^{n+1} \end{aligned}$$

where

1. $t_1 = 1,\ t_2 = -c_1/2$;

2. *for each* i, it_i *is a polynomial in* c_1, c_2, c_3, c_4, c_6 *with integral coefficients;*

3. t_i *is of weight* i.

Proof ▶ Since

$$\begin{aligned}\frac{d\theta}{dX} &= \frac{1}{1 + c_1X + 2c_3Z - c_2X^2 - 2c_4XZ - 3c_6Z^2} \\ &= 1 - (c_1X + 2c_3Z - c_2X^2 - 2c_4XZ - 3c_6Z^2) \\ &\qquad + (c_1X + 2c_3Z - c_2X^2 - 2c_4XZ - 3c_6Z^2)^2 + \cdots\end{aligned}$$

the coefficients in the power-series for $d\theta/dX$ are integral polynomials in the c_i. It follows on integration that the coefficients t_i in the power-series for $\theta(X)$ have at worst denominator i.

It remains to show that this power series converges for $\|X\|_p < 1$.

Lemma 6 *For all* i,

$$\|1/i\|_p \le i.$$

Proof of Lemma ▷ Suppose

$$\|i\|_p = p^{-e}.$$

Then

$$\begin{aligned}p^e \mid i &\Longrightarrow p^e \le i \\ &\Longrightarrow \|1/i\| \le i.\end{aligned}$$

◁

If now $\|X\|_p < 1$ then

$$\|X\|_p \le \frac{1}{p};$$

and so

$$\|t_iX^i\|_p \le \frac{i}{p^i},$$

which tends to 0 as $i \to \infty$. The power-series is therefore convergent. ◀

Note that

$$p^i \ge 2^i = (1+1)^i > i^2/2$$

if $i \ge 2$, while if p is odd, $\|1/2\|_p = 1$. Thus

$$\begin{aligned}\|X\|_p \le p^{-1} &\Longrightarrow \|X^i/i\|_p \le p^{-2} \text{ for } i \ge 2 \qquad (p \text{ odd}) \\ \|X\|_2 \le 2^{-2} &\Longrightarrow \|X^i/i\|_2 \le 2^{-3} \text{ for } i \ge 2 \qquad (p = 2).\end{aligned}$$

So if p is odd,

$$\theta(X) = X + O(p^2) \text{ if } \|X\|_p \le p^{-1};$$

while if $p = 2$,

$$\theta(X) = X + O(2^3) \text{ if } \|X\|_2 \leq 2^{-2}.$$

That is why in our discussion below the argument often applies to $P \in \mathcal{E}_{(p)}$ if p is odd, while if $p = 2$ we have to restrict P to $\mathcal{E}_{2^2}$.

Theorem 6.1 *For each power p^e, where $e \geq 1$,*

$$\mathcal{E}_{(p^e)}(\mathbb{Q}_p)$$

is a subgroup of $\mathcal{E}(\mathbb{Q}_p)$. Moreover the map

$$\theta : \mathcal{E}_{(p^e)}(\mathbb{Q}_p) \to p^e\mathbb{Z}_p$$

is an isomorphism (of topological abelian groups), provided $e \geq 2$ if $p = 2$.

Proof ▶ The identity

$$\theta(S(X_1, X_2) = \theta(X_1) + \theta(X_2),$$

which we established in the real case, must still hold; and we conclude from it, as before, that

$$\theta(P_1 + P_2) = \theta(P_1) + \theta(P_2)$$

whenever

$$P_1, P_2 \in \mathcal{E}_{(p^e)}(\mathbb{Q}_p).$$

It follows from this that $\mathcal{E}_{(p^e)}$ is a subgroup; and that

$$\theta : \mathcal{E}_{(p^e)} \to p^e\mathbb{Z}_p$$

is a homomorphism, provided $e \geq 2$ if $p = 2$.

Since

$$\theta(X) = X - c_1X^2/2 + \cdots,$$

we have

$$\|\theta(X)\|_p = \|X\|_p$$

for all $\|X\|_p \leq p^{-e}$. In particular

$$\theta(X) = 0 \Longleftrightarrow X = 0.$$

Hence θ is injective.

It is also surjective, as the following Lemma will show.

Lemma 7 *The only closed subgroups of $\mathbb{Z}_p$ are the subgroups*

$$p^n\mathbb{Z}_p \quad (n = 0, 1, 2, \ldots),$$

together with $\{0\}$. In particular, every closed subgroup of $\mathbb{Z}_p$, apart from $\{0\}$, is in fact open.

Proof of Lemma ▷ $\mathbb{Z}$ is a dense subset of $\mathbb{Z}_p$:

$$\overline{\mathbb{Z}} = \mathbb{Z}_p.$$

For the p-adic integer

$$x = c_0 + c_1 p + c_2 p^2 + \cdots \quad (c_i \in \{0, 1, \ldots, p-1\})$$

is approached arbitrarily closely by the (rational) integers

$$x_r = c_0 + c_1 p + \cdots + c_r p^r.$$

Now suppose S is a closed subgroup of $\mathbb{Z}_p$. Let $s \in S$ be an element of maximal p-adic valuation, say

$$\|s\| = p^{-e}.$$

Then

$$s = p^e u$$

where u is a unit in $\mathbb{Z}_p$, with inverse v, say. Given any $\epsilon > 0$, we can find $n \in \mathbb{Z}$ such that

$$\|v - n\| < \epsilon.$$

Then

$$\begin{aligned} ns - p^e &= p^e(nu - 1) \\ &= p^e u(n - v); \end{aligned}$$

and so

$$\|ns - p^e\| < \epsilon.$$

Since $ns \in S$ and S is closed, it follows that

$$p^e \in S.$$

Hence

$$p^e \overline{\mathbb{Z}} = p^e \mathbb{Z}_p \subset S.$$

Since s was a maximal element in S, it follows that

$$S = p^e \mathbb{Z}_p.$$

◁

It follows from this Lemma that $\operatorname{im}\theta$ is one of the subgroups $p^m\mathbb{Z}_p$. But since

$$\|X\| = p^{-e} \Longrightarrow \|\theta(X)\| = p^{-e},$$

$\operatorname{im}\theta$ must in fact be $p^e\mathbb{Z}_p$, ie θ is surjective.

A continuous bijective map from a compact space to a hausdorff space is necessarily a homeomorphism. (This follows from the fact that the image of every closed, and therefore compact, subset is compact, and therefore closed.) In particular, θ establishes an isomorphism

$$\mathcal{E}_{(p^e)} \cong p^e\mathbb{Z}_p \cong \mathbb{Z}_p.$$

◀

It follows from this Theorem that $\mathcal{E}_{(p^e)}$ is torsion-free, since $\mathbb{Z}_p$ is torsion-free. Thus *there are no points of finite order on $\mathcal{E}$ close to O*, a result which we shall exploit in the next Chapter.

6.4 The Structure of $\mathcal{E}(\mathbb{Q}_p)$

We shall not use the following result, but include it for the sake of completeness.

Theorem 6.2 *Let $\mathbb{F} \subset \mathcal{E}(\mathbb{Q}_p)$ be the torsion subgroup of the elliptic curve $\mathcal{E}(\mathbb{Q}_p)$. Then*

$$\mathcal{E}(\mathbb{Q}_p) \cong \mathbb{F} \oplus \mathbb{Z}_p.$$

Proof ► The torsion subgroup $\mathbb{F}$ splits (uniquely) into its p-component $\mathbb{F}_p$ and the sum $\mathbb{F}_{p'}$ of all components $\mathbb{F}_q$ with $q \neq p$:

$$\mathbb{F} = \mathbb{F}_p \oplus \mathbb{F}_{p'}.$$

(See Appendix A for details.) Explicitly,

$$\begin{aligned}\mathbb{F}_p &= \{P \in \mathcal{E} : p^n P = 0 \text{ for some } n\},\\ \mathbb{F}_{p'} &= \{P \in \mathcal{E} : mP = 0 \text{ for some } d \text{ with } \gcd(m,p) = 1\}.\end{aligned}$$

(We write $\mathcal{E}$ for $\mathcal{E}(\mathbb{Q}_p)$).

We also set

$$\mathcal{E}_p = \{P \in \mathcal{E} : p^n P \to O \text{ as } n \to \infty\}.$$

Evidently

$$\mathcal{E}_p \supset \mathcal{E}_{(p)}.$$

Since $E_{(p)}$ is an open (and therefore closed) subgroup of $\mathcal{E}$, it follows that the same is true of $\mathcal{E}_p$.

Lemma 8 $p^n \mathcal{E}_p = \mathcal{E}_{(p^e)}$ *for some $n, e > 0$.*

Proof of Lemma ▷ For each $P \in \mathcal{E}_p$,

$$p^n P \in \mathcal{E}_{(p)}$$

for some $n > 0$ since $p^n P \to O$ and $\mathcal{E}_{(p)}$ is an open neighbourhood of O. Hence the open subgroups $p^{-n}\mathcal{E}_{(p)}$ cover $\mathcal{E}_p$. Since $\mathcal{E}_p$ is compact, it follows that $p^{-n}\mathcal{E}_{(p)} \supset \mathcal{E}_p$ for some n, ie

$$p^n \mathcal{E}_p \subset \mathcal{E}_{(p)} \cong \mathbb{Z}_p.$$

But by Lemma 7 to Theorem 6.1, the only closed subgroups of $\mathbb{Z}_p$ are the $p^e Z_p$, which correspond under this isomorphism to the subgroups $\mathcal{E}_{(p^e)}$ of $\mathcal{E}_{(p)}$.

We conclude that

$$p^n \mathcal{E}_p = \mathcal{E}_{(p^e)}$$

for some e. ◁

Lemma 9 *Suppose A is a finite p-group; and suppose* $\gcd(m, p) = 1$. *Then the map $\psi : A \to A$ under which*

$$a \mapsto ma$$

is an isomorphism.

Proof of Lemma ▷ Suppose $a \in \ker A$, ie

$$ma = 0.$$

Then $\text{order}(a) \mid m$. But by Lagrange's Theorem, $\text{order}(a) = p^e$ for some e. Hence $order(a) = 1$, ie $a = 0$.

Thus ψ is injective; and it is therefore surjective, by the Pigeon-Hole Principle. Hence ψ is an isomorphism. ◁

It is not difficult to extend this result to $\mathcal{E}_p$, which is in effect a kind of topological p-group.

Lemma 10 *Suppose* $\gcd(m, p) = 1$. *Then the map $\psi : \mathcal{E}_p \to \mathcal{E}_p$ under which*

$$a \mapsto ma$$

is an isomorphism.

Proof of Lemma ▷ Suppose $P \in \ker \psi$, ie

$$mP = 0.$$

By Lemma 1,

$$p^n \mathcal{E}_p \subset \mathcal{E}_{(p^2)} \cong \mathbb{Z}_p$$

for some n.

But $\mathbb{Z}_p$ is torsion-free. Thus

$$mP = 0 \Longrightarrow m(p^n P = 0) \Longrightarrow p^n P = 0.$$

Hence

$$m, p^n \mid \text{order}(P) \Longrightarrow \text{order}(P) = 1 \Longrightarrow P = 0$$

since $\gcd(m, p^n) = 1$. Thus

$$\ker \psi = 0,$$

ie ψ is injective.

Now suppose $P \in \mathcal{E}_p$. We have to show that $P = mQ$ for some $Q \in \mathcal{E}_p$.

Since $\mathcal{E}_p / p^n \mathcal{E}_p$ is a finite p-group we can find $Q \in \mathcal{E}_p$ such that

$$mQ \equiv P \bmod p^n \mathcal{E}_p$$

ie

$$mQ = P + R,$$

where

$$R \in p^n \mathcal{E}_p \cong \mathbb{Z}_p.$$

Now the map

$$P \mapsto mP : \mathbb{Z}_p \to \mathbb{Z}_p$$

is certainly an isomorphism, since m is a unit in $\mathbb{Z}_p$ with inverse $m^{-1} \in \mathbb{Z}_p$. In particular we can find $S \in p^n \mathcal{E}_p$ with

$$mS = R.$$

Putting all this together,

$$P = mQ + R = mQ + mS = m(Q + S).$$

Thus the map ψ is surjective, and so an isomorphism. $\triangleleft$

Lemma 11 $\mathcal{E}(\mathbb{Q}_p) = \mathbb{F}_{p'} \oplus \mathcal{E}_p$.

Proof of Lemma $\triangleright$ Suppose

$$P \in \mathbb{F}_{p'} \cap \mathcal{E}_p,$$

say

$$mP = O,$$

where $\gcd(m, p) = 1$.

On considering $p \bmod m$ as an element of the finite group

$$(\mathbb{Z}/m)^\times = \{r \bmod m : \gcd(r, m) = 1\},$$

it follows by Lagrange's Theorem that

$$p^r \equiv 1 \bmod m$$

for some $n > 0$. But then

$$p^r P = P;$$

and so

$$p^n P \to O \implies P = O.$$

Now suppose $P \in \mathcal{E}$. Since $\mathcal{E}$ is compact, and $\mathcal{E}_p$ is open, $\mathcal{E}/\mathcal{E}_p$ is finite (eg since $\mathcal{E}$ must be covered by a finite number of $\mathcal{E}_p$-cosets). Let the order of this finite group be mp^e, where $\gcd(m, p) = 1$.

We can find $u, v \in \mathbb{Z}$ such that

$$um + vp^e = 1;$$

and then

$$P = Q + R,$$

where

$$Q = u(mP),\ R = v(p^e P).$$

Now

$$p^e Q = u(mp^e P) \in \mathcal{E}_p.$$

Hence

$$p^n Q \to 0 \text{ as } n \to \infty$$

ie

$$Q \in \mathcal{E}_p.$$

On the other hand,

$$mR = v(mp^e P) \in \mathcal{E}_p.$$

Hence by Lemma 10, there is a point $S \in \mathcal{E}_p$ such that

$$mR = mS,$$

and so

$$T = R - S \in \mathbb{F}_{p'}.$$

Putting these results together,

$$P = T + (Q + S),$$

with $T \in \mathbb{F}_{p'}$ and $Q + S \in \mathcal{E}_p$. $\triangleleft$

Lemma 12 $\mathbb{F}_p \subset \mathcal{E}_p$.

Proof of Lemma $\triangleright$ Suppose

$$P = Q + R \in \mathbb{F}_p,$$

where $Q \in \mathbb{F}_{p'},\ R \in \mathcal{E}_p$. Then

$$p^n P = 0 \Longrightarrow p^n Q = 0,\ p^n R = 0,$$

since the sum is direct. But

$$p^n Q = 0 \Longrightarrow \text{order}(Q) \mid p^n \Longrightarrow \text{order}(Q) = 1 \Longrightarrow Q = 0,$$

since the order of Q is coprime to p by the definition of $\mathbb{F}_{p'}$. Thus

$$P = R \in \mathcal{E}_p.$$

$\triangleleft$

It remains to split $\mathcal{E}_p$ into $\mathbb{F}_p$ and a subgroup isomorphic to $\mathbb{Z}_p$.

Consider the surjection

$$\psi : \mathcal{E}_p \to \mathcal{E}_{(p^e)} \cong \mathbb{Z}_p.$$

Let us choose a point

$$P_0 \in \mathcal{E}_{p^e} \setminus \mathcal{E}_{(p^{e+1})},$$

eg if we identify $\mathcal{E}_{(p^e)}$ with $\mathbb{Z}_p$ we might take the point corresponding to $1 \in \mathbb{Z}_p$. Now choose a point P_1 such that

$$\psi(P_1) = P_0;$$

and let

$$\mathcal{E}_1 = \overline{\langle P_1 \rangle}$$

be the closure in $\mathcal{E}_p$ of the subgroup generated by P_1. We shall show that the restriction

$$\psi_1 = \psi \mid \mathcal{E}_1 : \mathcal{E}_1 \to \mathcal{E}_{(p^e)}$$

is an isomorphism, so that

$$\mathcal{E}_1 \cong \mathcal{E}_{(p^e)} \cong \mathbb{Z}_p.$$

Certainly ψ_1 is surjective. For $\mathcal{E}_1$ is compact, and so its image is closed; while $\langle P_0 \rangle >$ is dense in $\mathcal{E}_{(p^e)} \cong \mathbb{Z}_p$.

Suppose

$$Q \in \ker \psi_1 = \ker \psi \cap \mathcal{E}_1.$$

By definition, Q is the limit of points in $\langle P_1 \rangle$, say

$$n_i P_1 \to Q,$$

where $n_i \in \mathbb{Z}$. But then, since ψ is continuous,

$$n_i P_0 \to \psi(Q) = 0.$$

Hence

$$n_i \to 0$$

in $\mathbb{Z}_p$. But then it follows that

$$n_i P_1 \to 0$$

in $\mathcal{E}_p$, since

$$\bigcap p^n E_p = 0.$$

Hence $Q = 0$, ie $\ker \psi_1 = 0$.

It remains to show that

$$\mathcal{E}_p = \mathbb{F}_p \oplus \mathcal{E}_1.$$

Suppose $P \in \mathcal{E}_p$. Then

$$\psi(P) = \psi(Q),$$

for some $Q \in \mathcal{E}_1$. In other words,

$$p^n(P - Q) = 0.$$

Thus

$$R = P - Q \in \mathbb{F}_p$$

On the other hand, if

$$F_p \cap \mathcal{E}_1 = 0,$$

since as we have seen,

$$\mathcal{E}_1 \cong \mathcal{E}_{(p^e)} \cong \mathbb{Z}_p,$$

and Z_p is torsion-free.

We have shown therefore that

$$\begin{aligned}
\mathcal{E} &= \mathbb{F}_{p'} \oplus \mathcal{E}_p \\
&= \mathbb{F}_{p'} \oplus (\mathbb{F}_p \oplus \mathcal{E}_1) \\
&= (\mathbb{F}_{p'} \oplus \mathbb{F}_p) \oplus \mathcal{E}_1 \\
&= \mathbb{F} \oplus \mathcal{E}_1 \\
&\cong \mathbb{F} \oplus \mathbb{Z}_p.
\end{aligned}$$

◀

Remark: We can regard $\mathcal{E}_p$ *as a* $\mathbb{Z}_p$*-module*; for since $p^n P \to O$ we can define xP unambiguously for $x \in \mathbb{Z}_p$:

$$n_i \to x \implies n_i P \to xP.$$

Moreover, $\mathcal{E}_p$ is a *finitely-generated* $\mathbb{Z}_p$-module; that follows readily from the fact that $\mathcal{E}_{(p)} \cong \mathbb{Z}_p$ is of finite index in $\mathcal{E}_p$.

The Structure Theorem for finitely-generated abelian groups, ie Z-modules, extends easily to $\mathbb{Z}_p$-modules; such a module is the direct sum of copies of $\mathbb{Z}_p$ and cyclic groups $\mathbb{Z}/(p^e)$. (This can be proved in much the same way as the corresponding result for abelian groups.)

Effectively, therefore, all we proved above was that the factor $\mathbb{Z}_p$ occurred just once, which simply reflects the fact that we are dealing with a 1-dimensional curve.