university of groningen

Bachelor's Project Mathematics

Non-Existence of Elliptic Curves over $\mathbb{Q}$ with Good Reduction Everywhere over Quadratic Fields

Briana–Mihaela Balea S5310423
b.m.balea@student.rug.nl

Supervisor I: Dr. Pınar Kılıçer
Supervisor II: Dr. Ekin Özman

Abstract

This thesis investigates the minimal field extensions over which elliptic curves defined over $\mathbb{Q}$ acquire good reduction everywhere. While it is a classical result due to Tate that no elliptic curve over $\mathbb{Q}$ admits good reduction at all primes, a natural question arises: Can good reduction everywhere be achieved over a quadratic extension of $\mathbb{Q}$? We review and present in detail a theorem of Kida, which gives a negative answer to this question. To this end, we develop the necessary arithmetic background, including valuations, ramification theory, and the study of elliptic curves in both local and global settings. We analyze how reduction behavior is influenced by field extensions, and establish criteria for when good reduction occurs. Finally, we provide explicit examples of elliptic curves that achieve good reduction everywhere over number fields of degrees 3, 4 and 6, illustrating the connection between local invariants and the specific nature of the required field extensions.

Contents

1 Introduction **4**

2 Number Fields **5**

2.1 Trace, norm and discriminant 6

2.2 Ramification 10

3 Local fields **11**

3.1 Absolute values and valuations 11

3.2 Completions 15

3.3 p-adic numbers and p-adic integers 17

3.4 Local fields 22

3.4.1 Extensions and ramification 23

3.4.2 Ramified and unramified quadratic extensions of $\mathbb{Q}_p$ 24

4 Elliptic Curves **28**

4.1 Legendre form 38

4.2 The Abelian Group of Elliptic Curves 39

4.3 Base change and twist 43

4.4 Elliptic curves over local fields 45

4.4.1 The Minimal Weierstrass Equation 45

4.4.2 Reduction 48

5 Acquiring good reduction **53**

5.1 Minimal degree of local extension for potential good reduction 54

5.2 Good reduction everywhere over quadratic fields 56

5.3 Examples: Good reduction everywhere 62

5.3.1 Cubic fields 62

5.3.2 Quartic Fields 63

5.3.3 Sextic Fields 63

1 Introduction

An elliptic curve is defined as a smooth projective curve given by a Weierstrass equation, together with a distinguished point at infinity. These curves have important arithmetic properties and appear naturally in number theory, as well as areas such as cryptography, coding theory and the study of Diophantine equations. A central theme in the arithmetic of elliptic curves is understanding how their properties vary over different fields, in particular, how they behave under reduction at primes of a number field.

One fundamental arithmetic invariant of an elliptic curve is its discriminant. The fact that an elliptic curve is nonsingular implies that its discriminant must be nonzero. When working over a local field, such as $\mathbb{Q}_p$, the field of p-adic numbers, we can consider a minimal Weierstrass equation, and reduce the equation modulo the maximal ideal. If the resulting curve over the residue field remains nonsingular, that is, its reduced discriminant is nonzero, we say that the elliptic curve has good reduction. On the other hand, if the reduction yields a singular curve, the curve has bad reduction. Globally, an elliptic curve over $\mathbb{Q}$ is said to have good reduction everywhere if it has good reduction at all primes p. This means that for every prime p, the base change of the curve to the local field $\mathbb{Q}_p$ has good reduction. Thus, determining whether a curve has good reduction everywhere globally requires checking its reduction behavior locally at each prime.

This thesis explores a natural but subtle question in the arithmetic of elliptic curves:

Given an elliptic curve over $\mathbb{Q}$, what is the minimal degree of a number field extension over which the curve acquires good reduction at all primes?

It is a well-known result by Tate that no elliptic curve defined over $\mathbb{Q}$ has good reduction everywhere (see [7], page 144). This leads to the question of whether such a curve might acquire good reduction everywhere over a quadratic extension of $\mathbb{Q}$. The answer is negative, as shown by Kida in [4], and in this paper we review his result in detail. Moreover, we examine some explicit examples of elliptic curves that do acquire good reduction everywhere over number fields of higher degree, and we relate the minimal degree of such fields to the arithmetic properties of the curve.

To understand Kida's result, we first turn to Section 2, where we review concepts from the theory of number fields, such as trace, norm, and discriminant, and introduce the notion of ramification. In Section 3, we move on to local fields and develop the necessary tools to analyze the local behavior of elliptic curves. This includes valuations, completions, and the structure of discrete valuation rings, with a focus on p-adic numbers. Section 4 introduces elliptic curves in detail, discusses minimality of their equations over local fields, and most importantly, their reduction. These concepts are then applied in Section 5, where we first study the local behavior of elliptic curves under base change in Section 5.1, specifically on the minimal degree of an extension of $\mathbb{Q}_p$ over which a curve with bad reduction at p acquires good reduction. We then shift our attention to the global setting in Section 5.2, where we review Kida's proof that good reduction cannot occur over quadratic fields for an elliptic curve defined over $\mathbb{Q}$. Finally, in Section 5.3, we provide minimal degree examples where good reduction everywhere is achieved over fields of degrees 3, 4 and 6.

We present a self-contained and accessible account of Kida's result, and illustrate how the arithmetic of elliptic curves influences the degrees of the fields over which good reduction everywhere can occur.

2 Number Fields

An *algebraic number field* is a finite extension of the field of rational numbers $\mathbb{Q}$. That is, a field K is called a number field if there exists a finite degree $n = [K : \mathbb{Q}]$ such that $\mathbb{Q} \subset K \subset \bar{\mathbb{Q}}$, where $\bar{\mathbb{Q}}$ is defined to be the algebraic closure of $\mathbb{Q}$.

In this section, we introduce the essential arithmetic invariants associated to number fields: trace, norm, and discriminant.

Definition 2.1 (Algebraic integers)**.** *Let $K/\mathbb{Q}$ be a finite extension. An element $\alpha \in K$ is called an* algebraic integer *if it is the root of a monic polynomial with coefficients in $\mathbb{Z}$.*

Definition 2.2 (Ring of integers)**.** *The* ring of integers *of K, denoted $\mathcal{O}_K$, is the set of all algebraic integers in K:*

$$\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}.$$

The ring $\mathcal{O}_K$ plays an essential role in the arithmetic of number fields. It is **integrally closed** in K, meaning that any element of K that satisfies a monic polynomial with coefficients in $\mathbb{Z}$ must already lie in $\mathcal{O}_K$. Moreover, it is a Dedekind domain, meaning that

- It is Noetherian, that is, every ideal is finitely generated;
- Every nonzero prime ideal is maximal;
- Every nonzero ideal factors uniquely into a product of prime ideals.

This last property generalizes the notion of unique factorization of numbers to the setting of ideals.

Notably, the ring $\mathbb{Z}[\sqrt{d}]$, with $d \in \mathbb{Z}$ squarefree, is not always integrally closed, i.e., not the ring of integers of $\mathbb{Q}(\sqrt{d})$, and in particular, not a Dedekind domain.

Example 2.3. *Consider $K = \mathbb{Q}(\sqrt{5})$. The subring $\mathbb{Z}[\sqrt{5}]$ is not the full ring of integers: it is not integrally closed and fails to be a Dedekind domain.*

To see this, consider $6 \in \mathbb{Z}[\sqrt{5}]$, and note the following:

$$6 = 2 \cdot 3 = (1 - \sqrt{5})(1 + \sqrt{5}).$$

Hence, 6 admits two distinct factorizations in $\mathbb{Z}[\sqrt{5}]$, as all four elements are irreducible.

The correct ring of integers of $\mathbb{Q}(\sqrt{5})$ is actually $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, which is indeed a Dedekind domain. We revisit this in Example 2.5.

Definition 2.4 (Integral basis)**.** *Let $K/\mathbb{Q}$ be a number field of degree n. A set $\{x_1, \ldots, x_n\} \subset \mathcal{O}_K$ is called an* integral basis *if every element $\alpha \in \mathcal{O}_K$ can be written uniquely as*

$$\alpha = a_1 x_1 + \cdots + a_n x_n, \quad a_i \in \mathbb{Z}.$$

Example 2.5. *Consider a number field $K := \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is square-free. Then, an integral basis for K is*

$$\begin{cases} \left\{1, \dfrac{1+\sqrt{d}}{2}\right\} & \text{if } d \equiv 1 \pmod 4 \\ \{1, \sqrt{d}\} & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \end{cases}$$

To see this, let $\alpha \in \mathcal{O}_K \subset K$. Then we must have

$$\alpha = \frac{a + b\sqrt{d}}{c}, \qquad a, b, c \in \mathbb{Z}$$

and we can assume without loss of generality that $\gcd(a, b, c) = 1$, i.e. that a, b, c are coprime. Then the minimal polynomial of α is given by

$$x^2 - \frac{2a}{c}x + \frac{a^2 - db^2}{c^2} \in \mathbb{Z}[x]$$

Now, if $\gcd(a, b) = m$, then from the constant term, it must be that $m \mid c$ as d is square-free, which we cannot have by assumption. Hence, $\gcd(a, b) = 1$. From the linear coefficient, we need $c \mid 2a$. Assume that $c \mid a$ and $c \neq 1$. Then we need $c^2 \mid db^2$ and since d is square-free, $c \mid b$, again, a contradiction, so $c \mid 2$, i.e., $c = 2$ or $c = 1$. If $c = 2$, we have

$$4 \mid a^2 - db^2 \iff a^2 - db^2 \equiv 0 \pmod 4 \iff a^2 \equiv db^2 \pmod 4$$

Now, we know that $2 \nmid a$, so clearly $4 \nmid a$, hence $a^2 \equiv 1 \pmod 4$, since the quadratic residues modulo 4 are 0 and 1, which yields

$$db^2 \equiv 1 \pmod 4.$$

From the above, we can only have that $b^2 \equiv 1 \pmod 4$ and so, $d \equiv 1 \pmod 4$ since d is square-free.

Therefore, when $d \equiv 1 \pmod 4$, an integral basis for K is

$$\left\{1, \frac{1+\sqrt{d}}{2}\right\}.$$

If $c = 1$, then $\alpha = a + b\sqrt{d}$, hence, an integral basis in this case is

$$\{1, \sqrt{d}\}.$$

Thus, the above also gives

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Recall that we previously claimed in Example 2.3 that the ring of integers of $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Indeed, we have that $5 \equiv 1 \pmod 4$, which proves our claim.

2.1 Trace, norm and discriminant

Let L/K be an extension of algebraic number fields. Each element $x \in L$ determines a K-linear map $r_x : L \to L$ given by

$$r_x(y) = xy, \quad \text{for all } y \in L.$$

This map can be represented as a matrix $|a_{ij}|$ after having chosen a basis $u_1, \ldots, u_n$ for the extension L over K so that

$$u_i x = \sum a_{ij} u_j.$$

Note that the functions $\mathrm{Tr}(|a_{ij}|)$ and $\det(|a_{ij}|)$ are independent of the choice of basis and only depend on the linear transformation r_x, i.e., only on x. With this in hand, we define two important functions associated with this representation:

Definition 2.6 (Trace and norm)**.** *The* trace *of x with respect to L/K, denoted $\mathrm{Tr}_{L/K}(x)$, is defined as the trace of the linear map r_x, that is,*

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(r_x).$$

The norm *of x with respect to L/K, denoted $\mathrm{N}_{L/K}(x)$, is defined as the determinant of r_x:*

$$\mathrm{N}_{L/K}(x) = \det(r_x).$$

The trace and norm have several important properties. Let $x, y \in L$ and $a \in K$. Then, the following hold:

1. **Additivity of Trace:** $\mathrm{Tr}_{L/K}(x+y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$.
2. **Homogeneity of Trace:** $\mathrm{Tr}_{L/K}(ax) = a\,\mathrm{Tr}_{L/K}(x)$.
3. **Multiplicativity of Norm:** $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\,\mathrm{N}_{L/K}(y)$.
4. **Homogeneity of Norm:** $\mathrm{N}_{L/K}(ax) = a^{[L:K]}\,\mathrm{N}_{L/K}(x)$.

The proof of these properties is quite straightforward if we recall that r_x is a K-linear map and hence

$$r_{xy} = r_x r_y \qquad \text{and} \qquad r_{x+y} = r_x + r_y,$$

and moreover, for any $m \times m$ matrices A and B over L and some scalar $a \in K$ one has

$$\mathrm{Tr}(aA + B) = a\,\mathrm{Tr}(A) + \mathrm{Tr}(B) \qquad \text{and} \qquad \det(aAB) = a^m \det(A)\det(B).$$

Furthermore, the trace has a transitive property. Let $K \subseteq E \subseteq L$ be a chain of finite extensions. Then for any $x \in L$, $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}(x))$.

Proof. Consider $a_1, \ldots, a_k$, a basis of E over K, and $b_1, \ldots, b_n$, a basis of L over E. Define

$$xb_i = \sum \beta_{ij}(x) b_j \qquad \text{and} \qquad ya_i = \sum \alpha_{ij}(y) a_j$$

for $x \in L$ and $y \in E$. Thus,

$$\mathrm{Tr}_{E/K} = \sum \alpha_{ii}(y) \qquad \text{and} \qquad \mathrm{Tr}_{L/E}(x) = \sum \beta_{ii}(x),$$

so from the above one obtains

$$\mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}) = \sum \sum \alpha_{ii}\left(\beta_{jj}(x)\right).$$

Now, the products $a_i b_j$ give a basis for L over K and

$$\begin{aligned} x a_s b_t &= \sum_j a_s \beta_{tj}(x) b_j \\ &= \sum_j \sum_i \alpha_{si}\left(\beta_{ij}(x)\right) a_i b_j \end{aligned}$$

which gives $\mathrm{Tr}_{L/K}(x) = \sum\sum \alpha_{ii}\left(\beta_{jj}(x)\right)$ whence

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}(x))$$

as needed. □

The *characteristic polynomial* of $x \in L$ over K is defined as $f_x(t) = \det|tI - r_x|$, which is a monic polynomial of degree $[L:K]$ with $f(r_x) = 0$, and so $f(x) = 0$. The discriminant of an extension L/K is defined in terms of the trace form, a symmetric bilinear form defined as follows:

Definition 2.7 (Discriminant, version I)**.** *The* bilinear form *of the extension L/K is the symmetric bilinear map $B : L \times L \to K$ defined by $B(x,y) = \mathrm{Tr}_{L/K}(xy)$. The* discriminant $\Delta_{L/K}$ *of the basis $x_1, \ldots, x_n$ of L/K is the determinant of the matrix of this bilinear form with respect to any basis of L/K, i.e.*

$$\Delta_{L/K}(x_1, \ldots, x_n) = \det|\,\mathrm{Tr}(x_i x_j)|$$

Additionally, we now consider L to be a separable extension of K.

Definition 2.8 (K-embedding)**.** *A* K-embedding *of L is a field homomorphism $\sigma : L \to \bar{K}$.*

Note that since σ is a field homomorphism from L to $\bar{K}$, it must be injective. To see this, assume $0 \neq a \in \ker(\sigma)$. Then,

$$0 = \sigma(a)\sigma(a^{-1}) = \sigma(aa^{-1}) = \sigma(1) = 1$$

which is clearly a contradiction hence σ must be injective. We also note that the restriction of σ to the base field K is precisely the identity map by the properties of field homomorphisms.

Proposition 2.9. *If L/K is a separable extension and $\sigma : L \to \bar{K}$ varies over the different K-embeddings of L into some algebraic closure of K, then*

(i) $f_x(t) = \prod_\sigma (t - \sigma x)$,

(ii) $\mathrm{Tr}_{L/K}(x) = \sum_\sigma \sigma x$,

(iii) $N_{L/K}(x) = \prod_\sigma \sigma x$

Proof. Recall that the characteristic polynomial $f_x(t)$ is a power of the minimal polynomial of x,

$$p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m, \qquad m = [K(x) : K].$$

We will show this and in fact,

$$f_x(t) = p_x(t)^d, \qquad d = [L : K(x)].$$

We have that $1, x, \ldots, x^{m-1}$ is a basis for $K(x)$ over K and let $a_1, \ldots, a_d$ be a basis for $L/K(x)$. Then,

$$\alpha_1, \alpha_1 x, \ldots, \alpha_1 x^{m-1}, \ldots, \alpha_d, \ldots, \alpha_d x^{m-1}$$

is a basis for L/K. The matrix of the linear map r_x with respect to this basis has then d blocks along the diagonal of the form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{pmatrix}$$

each with characteristic polynomial $p_x(t)$ hence, indeed $f_x(t) = p_x(t)^d$.

Now, consider the set of all K-embeddings of L, $\mathrm{Hom}_K(L, \bar{K})$. This set can be partitioned by the equivalence relation

$$\sigma \sim \tau \quad \Longleftrightarrow \quad \sigma x = \tau x$$

into m equivalence classes of d elements each. Let $\sigma_1, \ldots, \sigma_m$ is a system of representatives, then

$$p_x(t) = \prod_{i=1}^{m} (t - \sigma_i x)$$

hence

$$f_x(t) = \prod_{i=1}^{m} (t - \sigma_i x)^d = \prod_{i=1}^{m} \prod_{\sigma \sim \sigma_i} (t - \sigma x) = \prod_{\sigma} (t - \sigma x).$$

This proves *(i)*, and by noting that $\mathrm{Tr}_{L/K}(x)$ is the coefficient of t^{n-1} in f_x and $N_{L/K}(x)$ is the coefficient of t^0, *(ii)* and *(iii)* follow. □

With the above proposition in hand, we can define the discriminant of some extension as follows.

Definition 2.10 (Discriminant, version II)**.** *Let L/K be a finite extension. The* discriminant $\Delta_{L/K}$ *of the basis $x_1, \ldots, x_n$ of L/K is given by*

$$\Delta_{L/K}(x_1, \ldots, x_n) = \det |\, \mathrm{Tr}_{L/K}(xy)| = \det(\sigma_i(x_j))^2$$

where $\sigma_i \in \mathrm{Hom}_K(L, \bar{K})$.

Definition 2.11. *The discriminant of L/K is the ideal $\Delta_{L/K} \leqslant O_K$ generated by $\Delta_{L/K}(x_1, \ldots, x_n)$ for all choices of $x_1, \ldots, x_n \in O_K$.*

Example 2.12. *For the quadratic number field $K = \mathbb{Q}(\sqrt{d})$, we have*

$$\Delta_{K/\mathbb{Q}} = \begin{cases} d, & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \end{cases}.$$

Note that the two embeddings of K are given by

$$\sigma_1 : \sqrt{d} \mapsto \sqrt{d}$$
$$\sigma_2 : \sqrt{d} \mapsto -\sqrt{d}$$

since for all $a \in \mathbb{Q}$, $\sigma_i(a) = a$.

From example 2.5 we know that a basis for $\mathcal{O}_K$ is given by

$$\left\{1, \frac{1+\sqrt{d}}{2}\right\} \text{ if } d \equiv 1 \pmod 4$$
$$\{1, \sqrt{d}\} \text{ if } d \equiv 2 \text{ or } 3 \pmod 4.$$

Let us first consider the case when $d \equiv 1 \pmod 4$. Compute:

$$\sigma_1\left(\frac{1+\sqrt{d}}{2}\right) = \frac{1+\sqrt{d}}{2};$$
$$\sigma_2\left(\frac{1+\sqrt{d}}{2}\right) = \frac{1-\sqrt{d}}{2}.$$

From the definition above we have

$$\Delta_{K/\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{vmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{vmatrix}^2 = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = \frac{1}{4}(1 - \sqrt{d} - 1 - \sqrt{d})^2 = d$$

hence $\Delta_{K/\mathbb{Q}}$ is the ideal generated by d.

Similarly, we consider $d \equiv 2$ or $3 \pmod 4$. Then we have

$$\Delta_{L/\mathbb{Q}}(1, \sqrt{d}) = \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d$$

so $\Delta_{K/\mathbb{Q}}$ is the ideal generated by $4d$.

2.2 Ramification

For a number field K, we define what it means for some extension of K to be ramified.

Definition 2.13 (Ramification)**.** *Let L/K be a finite extension of number fields. A nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is said to be ramified in L if the ideal $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$ factors in primes as*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$$

where $e_i > 1$ for some i. We call e_i the ramification index for $\mathfrak{P}_i/\mathfrak{p}$, denoted by $e_i = e(\mathfrak{P}_i/\mathfrak{p})$.

Remark 2.14. *The ideal $\mathfrak{p}\mathcal{O}_L$ factors uniquely in L, as we have seen in the beginning of Section 2 that it is a Dedekind domain.*

In the case that $e(\mathfrak{P}_i/\mathfrak{p}) = 1$ for all i, we say that $\mathfrak{p}$ is unramified in L/K and totally ramified if $e(\mathfrak{P}/\mathfrak{p}) = [L : K]$ for a unique prime $\mathfrak{P}$.

Theorem 2.15. *The prime $\mathfrak{p}$ ramifies in L if and only if $\mathfrak{p} \mid \Delta_{L/K}$.*

Proof. See Corollary 2.12 in [6]. □

Example 2.16. *For $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, with d square-free, $d \equiv 2$ or $3 \pmod 4$, the prime 2 ramifies in $\mathbb{Q}(\sqrt{d})$. Indeed, from previous examples we have*

$$\Delta_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} = 4d$$

hence $2 \mid \Delta_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}$. Moreover, every prime dividing d ramifies in $\mathbb{Q}(\sqrt{d})$.

3 Local fields

3.1 Absolute values and valuations

Definition 3.1 (Absolute value)**.** *An* absolute value *on a field K is a function $|\cdot| : K \to \mathbb{R}_{\geqslant 0}$ satisfying:*

1. $|x| = 0$ *if and only if* $x = 0$*;*
2. $|xy| = |x| \cdot |y|$ *for all* $x, y \in K$*;*
3. $|x + y| \leqslant |x| + |y|$ *for all* $x, y \in K$*.*

The absolute value is called non-archimedean *if it satisfies the stronger triangle inequality:*

$$|x + y| \leqslant \max\{|x|, |y|\},$$

and archimedean *otherwise.*

Example 3.2. *The usual absolute value $|\cdot|_\infty$ on $\mathbb{Q}$, defined by $|x|_\infty = |x|$, is archimedean. Indeed, $|\cdot|_\infty$ does not satisfy the strong triangle inequality. Take, for example, $x = y = 1$, then*

$$|1 + 1| = 2 \geqslant 1 = \max\{1, 1\}.$$

For a prime number p, the p-adic absolute value on $\mathbb{Q}$ is defined by:

$$|x|_p = \begin{cases} p^{-n} & \text{if } x = p^n \frac{a}{b} \text{ with } \gcd(a, b) = 1 \text{ and } a, b \in \mathbb{Z},\ p \nmid a, b, \\ 0 & \text{if } x = 0. \end{cases}$$

This absolute value is non-archimedean. To see this, let $x, y \in \mathbb{Q}\backslash\{0\}$. Then, we can write

$$x = p^n \frac{a}{b} \qquad \text{and} \qquad y = p^m \frac{c}{d}, \qquad \text{where } a, b, c, d \in \mathbb{Z} \text{ and } p \nmid a, b, c, d.$$

Assume without loss of generality that $n \geqslant m$. Hence, we have

$$|x + y|_p = \left|p^n \frac{a}{b} + p^m \frac{c}{d}\right|_p = |p^m|_p \left|p^{n-m} \frac{a}{b} + \frac{c}{d}\right|_p \leqslant |p^m|_p = p^{-m} = |y|_p = \max\{|x|_p, |y|_p\}.$$

Definition 3.3 (Valuation)**.** *A (real)* valuation *on K is a function $v : K^\times \to \mathbb{R}$ satisfying:*

(a) $v(xy) = v(x) + v(y)$*;*

(b) $v(x + y) \geqslant \min\{v(x), v(y)\}$ *for all* $x, y \in K^\times$*.*

We define $v(0) = \infty$ by convention.

Definition 3.4 (Discrete valuation)**.** *A valuation v is called* discrete *if its image is $\mathbb{Z}$. That is, $v : K^\times \to \mathbb{Z}$ is a surjective homomorphism satisfying the same properties as above.*

Example 3.5. *Let $K = \mathbb{Q}$, and let p be a prime number. Every nonzero rational number $x \in \mathbb{Q}^\times$ can be uniquely written in the form*

$$x = p^n \cdot \frac{a}{b},$$

where $a, b \in \mathbb{Z}$ and $p \nmid a, b$. This defines a discrete valuation

$$v_p(x) := n.$$

Before introducing the concept of a valuation ring we need the following definition.

Definition 3.6. *A ring having only one maximal ideal is called a local ring.*

Definition 3.7 (Valuation ring)**.** *Let v be a discrete valuation on K. The* discrete valuation ring *associated to v is*

$$\mathcal{O}_K := \{x \in K : v(x) \geqslant 0\}.$$

We shall prove that $\mathcal{O}_K$, defined as above, is indeed a ring, and in fact, a subring of K.

Proposition 3.8. *Let K be a field and v, a discrete valuation on K. Then $\mathcal{O}_K$ defined as above is a subring of K. Moreover, the subset $\{x \in K : v(x) > 0\}$ is an ideal of $\mathcal{O}_K$ and $\mathcal{O}_K^\times = \{x \in K : v(x) = 0\}$.*

Proof. First, note that for all $x \in K^\times$ it holds that

$$v(x) = v(x \cdot 1) = v(x) + v(1) \quad \iff \quad v(1) = 0$$

and

$$v(1) = v((-1)\cdot(-1)) = v(-1) + v(-1) \iff 0 = 2v(-1) \iff v(-1) = 0.$$

Now, take x, $y \in \mathcal{O}_K$, then

$$v(x + y) \geqslant \min\{v(x), v(y)\} \geqslant 0$$

hence $x + y \in \mathcal{O}_K$ and

$$v(xy) = v(x) + v(y) \geqslant 0 \cdot 0 = 0$$

so, $xy \in \mathcal{O}_K$. Next, we show that $\{x \in K : v(x) > 0\} := I$. Indeed, let x, $y \in I$. Then, we have

$$v(x + y) \geqslant \min\{v(x), v(y)\} > 0$$

hence $x + y \in I$ and $v(0) > 0$, so $(I, +)$ is a subgroup of $(\mathcal{O}_K, +)$. Moreover, for $x \in I$ and $y \in \mathcal{O}_K$, we also have

$$v(xy) = v(x) + v(y) \geqslant v(x) + 0 > 0$$

thus $xy \in I$. This shows that I is indeed an ideal of $\mathcal{O}_K$.

Finally, we show that $\mathcal{O}_K^\times = \{x \in K : v(x) = 0\}$. Let $x \in \mathcal{O}_K^\times$ which holds if and only if $v(x) \geqslant 0$ and $v(x^{-1}) \geqslant 0$ so

$$0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) \quad \iff \quad v(x^{-1}) = -v(x) \geqslant 0 \quad \iff \quad v(x) = v(x^{-1}) = 0,$$

hence we are done. □

Proposition 3.9. *The valuation ring $\mathcal{O}_K$ is a local ring with maximal ideal*

$$\mathfrak{m} := \{x \in K : v(x) > 0\},$$

and residue field

$$k := \mathcal{O}_K/\mathfrak{m}.$$

Proof. The fact that $\mathcal{O}_K$ is a ring and that $\mathfrak{m}$ is an ideal we know from Proposition 3.8. It is left to show that $\mathfrak{m}$ is the unique maximal ideal of $\mathcal{O}_K$. First, we prove that it is maximal.

Suppose that there exists some ideal I such that

$$\mathfrak{m} \subset I \subset \mathcal{O}_K.$$

Take $x \in I$ such that $x \notin \mathfrak{m}$. Then we have $x \in I \subset \mathcal{O}_K$, hence $v(x) \geqslant 0$, but $x \notin \mathfrak{m}$, implying that $v(x) = 0$. Therefore, by Proposition 3.8, $x \in \mathcal{O}_K^\times$, and so, $I = \mathcal{O}_K$, a contradiction. Thus, $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}_K$.

Now, assume that J is some proper ideal of $\mathcal{O}_K$. Note that this implies that for all $x \in J$, $v(x) > 0$, since $v(x) = 0$ would yield that $J = \mathcal{O}_K$. But this implies precisely that $J \subseteq \mathfrak{m}$, showing uniqueness of$\mathfrak{m}$.

Finally, since $\mathfrak{m}$ is maximal, $\mathcal{O}_K/\mathfrak{m}$ is a field and we denote it by k. □

Definition 3.10 (Uniformizer)**.** *An element $\pi \in \mathcal{O}_K$ is called a* uniformizer *if $v(\pi) = 1$.*

Proposition 3.11. *For a local field K, some discrete valuation v on K and a uniformizer $\pi \in \mathcal{O}_K$, the maximal ideal of $\mathcal{O}_K$ can be generated by π, i.e., $\mathfrak{m} = (\pi)$.*

Proof. We shall prove that

$$\mathfrak{m} = (\pi).$$

First, let $x \in (\pi)$. Then, $x = \pi \cdot u$ for some $u \in \mathcal{O}_K$, so

$$v(x) = v(\pi \cdot u) = v(\pi) + v(u) = 1 + v(u) > 0$$

implying that $(\pi) \subseteq \mathfrak{m}$.

Now, let $x \in \mathfrak{m}$ and denote $v(x) = n > 0$. Since $v(\pi) = 1$, we can then write

$$x = \pi^n u, \qquad \text{for some } u \in K^\times$$

and so,

$$v(x) = v(\pi^n u) = v(\pi^n) + v(u) \iff v(u) = n - n = 0$$

hence $u \in \mathcal{O}_K^\times$. We can also write

$$x = \pi \cdot (\pi^{n-1} u)$$

and $\pi^{n-1} \in \mathcal{O}_K$, giving $x \in (\pi)$, thus $\mathfrak{m} \subseteq (\pi)$. □

Definition 3.12 (Discrete valuation ring (DVR))**.** *A* discrete valuation ring *is a principal ideal domain with a unique nonzero prime ideal. Equivalently, it is a ring that arises as the valuation ring of a discrete valuation on a field.*

Suppose now that v is a discrete valuation on some field K. Next, we introduce a couple definitions in order to establish an important property of the discrete valuation ring $\mathcal{O}_K$ of K.

Definition 3.13 (Integral element)**.** *Let A be an integral domain and K a field such that $A \subset K$. We say that $x \in K$ is* integral *over A if and only if there exists some monic polynomial $f(x) \in A[x]$ such that $f(x) = 0$.*

Definition 3.14 (Integral closure)**.** *Let A be an integral domain and K some field such that $A \subset K$. The* integral closure *of A in K is the set of all elements in K that are integral over A.*

We say that A is integrally closed if it contains all elements of its field of fractions that are integral over it.

Theorem 3.15. *Let A be a unique factorization domain and K its field of fractions. Then A is integrally closed.*

Proof. Since K is the field of fractions of A, for all $x \in K$ be integral over A write

$$x = \frac{a}{b}, \quad a, b \in A,$$

and we may assume without loss of generality that $\gcd(a, b) = 1$, that is, the ideal (a, b) is generated by 1. Note that we can do this since the greatest common divisor is well-defined in unique factorization domains and if $\gcd(a, b) = m$, there exist $c, d \in A$ with $\gcd(c, d) = 1$ such that

$$x = \frac{a}{b} = \frac{mc}{md} = \frac{c}{d}.$$

Then a/b is a root of some monic polynomial in $A[x]$

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0,$$

that is, we have

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_0 = 0$$

and multiplying the equality by b^n gives

$$a^n + bc = 0$$

for some $c \in A$, hence $b \mid a^n$. But, $\gcd(a, b) = 1$, so it must be that $b \in A^\times$. Therefore,

$$x = ab^{-1} \in A$$

showing that A is indeed integrally closed. □

We make the following claim:

Proposition 3.16. *If $\mathcal{O}_K$ is a discrete valuation ring of K, then it is integrally closed.*

Proof. First, note that the field of fractions of $\mathcal{O}_K$ is K. Indeed, since $\mathcal{O}_K \subset K$ and every $x \in K^\times$ is a quotient of two elements in $\mathcal{O}_K$.

Next, by definition, $\mathcal{O}_K$ is a principal ideal domain, and therefore a unique factorization domain. It then follows from the previous theorem that $\mathcal{O}_K$ is integrally closed. □

3.2 Completions

In this section, we consider a field K equipped with a valuation $v : K \to \mathbb{R}$. Associated to this valuation, we define the absolute value

$$|x| = c^{v(x)}$$

for some fixed constant $c > 1$. This absolute value is non-archimedean, and it directly inherits the properties of the valuation. For ease of notation, we will consistently use $|\cdot|$ in this section, while recognizing that this absolute value is derived from the underlying valuation v.

Consider the field K equipped with the valuation $|\cdot|$. We say that a sequence of elements $(a_n)_n$ in K is Cauchy if

$$\lim_{n,m\to\infty} |a_n - a_m| = 0.$$

Moreover, we say that $(a_n)_n$ converges to some element a (not necessarily of K) if

$$\lim_{n\to\infty} |a_n - a| = 0.$$

Definition 3.17. *A field K is* complete *with respect to the valuation $|\cdot|$ if every Cauchy sequence converges to an element of K.*

We define a relation on the set of Cauchy sequences in K as follows:

$$(x_n) \sim (y_n) \iff \lim_{n\to\infty} |x_n - y_n| = 0.$$

Proposition 3.18. *The relation $\sim$ is an equivalence relation.*

Proof. We verify the three properties:

- **Reflexivity:** For any Cauchy sequence (x_n), we have $|x_n - x_n| = 0$, so $(x_n) \sim (x_n)$.
- **Symmetry:** If $(x_n) \sim (y_n)$, then $|x_n - y_n| \to 0$ as $n \to \infty$. But by the symmetry of the valuation, $|y_n - x_n| = |x_n - y_n| \to 0$, so $(y_n) \sim (x_n)$.
- **Transitivity:** If $(x_n) \sim (y_n)$ and $(y_n) \sim (z_n)$, then

  $$|x_n - z_n| \leqslant |x_n - y_n| + |y_n - z_n| \to 0 + 0 = 0.$$

  where we used the triangle inequality. Therefore, $(x_n) \sim (z_n)$.

□

We write $[(x_n)]$ for the equivalence class of a Cauchy sequence (x_n).

Definition 3.19 (Completion of a field)**.** *The* completion *of K, denoted $\widehat{K}$, is defined as the set of equivalence classes of Cauchy sequences in K under this relation.*

In order for this definition to be valid we need to show that $\widehat{K}$ is a field and that it is also complete. To this end, recall the following properties of Cauchy Sequences:

1. If $(a_n)_n$ and $(b_n)_n$ are Cauchy, then so are $(a_n + b_n)_n$ and $(a_n b_n)_n$;
2. If $\lim |a_n| \neq 0$, then $a_n \neq 0$ for all $n \geqslant n_0$ for some n_0. In this case, $\left(a_n^{-1}\right)_n$ is Cauchy.

Then, we can define addition and multiplication in K as follows:

$$\begin{aligned}[(a_n)] + [(b_n)] &= [(a_n + b_n)];\\ [(a_n)][(b_n)] &= [(a_n b_n)];\\ [(a_n)]^{-1} &= [(a_n^{-1})] \quad \text{when } a_n^{-1} \text{ is defined.}\end{aligned}$$

In this case, we identify the 0 element with the equivalence class of Cauchy sequences converging to $0 \in K$, and the 1 element with the Cauchy sequences converging to $1 \in K$. Therefore, with these definitions, $\widehat{K}$ acquires the structure of a field. There is a natural embedding $K \hookrightarrow \widehat{K}$ sending each $x \in K$ to the constant sequence $(x, x, x, \dots)$. The valuation on K extends uniquely to $\widehat{K}$ by setting

$$|[(x_n)]| = \lim_{n\to\infty} |x_n|.$$

The above is actually a valuation on $\widehat{K}$ agreeing with the valuation on K. We first verify that this extended absolute value is well-defined: - If $(x_n) \sim (y_n)$, then by definition, $|x_n - y_n| \to 0$. Consequently,

$$\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |y_n|.$$

Thus, the absolute value is independent of the choice of representative in the equivalence class.

Next, we check that this defines a valuation:

- **Non-negativity:** By definition, $|[(x_n)]| \geqslant 0$. Moreover, $|[(x_n)]| = 0$ if and only if
$$\lim_{n\to\infty} |x_n| = 0,$$
which is true if and only if $[(x_n)]$ is the zero element of $\widehat{K}$ (the equivalence class of sequences converging to 0).
- **Multiplicativity:** Let $[(x_n)], [(y_n)] \in \widehat{K}$. Then:
$$|[(x_n)] \cdot [(y_n)]| = |[(x_n y_n)]| = \lim_{n\to\infty} |x_n y_n| = \lim_{n\to\infty} |x_n| \cdot |y_n|$$
which simplifies to
$$|[(x_n)]| \cdot |[(y_n)]|.$$
- **Non-archimedean property:** For $[(x_n)], [(y_n)] \in \widehat{K}$,
$$|[(x_n)] + [(y_n)]| = |[(x_n + y_n)]| = \lim_{n\to\infty} |x_n + y_n|.$$
Since the absolute value on K is non-archimedean,
$$|x_n + y_n| \leqslant \max\{|x_n|, |y_n|\}.$$
Taking the limit gives:
$$\lim_{n\to\infty} |x_n + y_n| \leqslant \max\left\{\lim_{n\to\infty} |x_n|, \lim_{n\to\infty} |y_n|\right\},$$
which is precisely:
$$|[(x_n)] + [(y_n)]| \leqslant \max\{|[(x_n)]|, |[(y_n)]|\}.$$

Finally, we show that this absolute value agrees with the valuation on K. If $x \in K$, we can view x as the constant sequence $(x, x, x, \ldots)$ in $\widehat{K}$. In this case:

$$|[(x)]| = \lim_{n\to\infty} |x| = |x|,$$

which is exactly the valuation-derived absolute value on K. Next, we show that $\widehat{K}$ is complete. Consider a Cauchy sequence in $[\alpha_n]$ $\widehat{K}$. Then, each α_n is a Cauchy sequence, say $\alpha_n = \left[\left(a_m^{(n)}\right)\right]$ in K, i.e., it is represented by the Cauchy sequence $\left(a_m^{(n)}\right)$ in K. Take α to be the sequence $\left[\left(a_m^{(m)}\right)\right]$. Note that we must have that (α_m) is Cauchy in K. Indeed,

$$\left|a_r^{(r)} - a_s^{(s)}\right| \leqslant \left|a_r^{(r)} - a_r^{(s)}\right| + \left|a_r^{(s)} - a_s^{(s)}\right|.$$

For some fixed s, $\left(a_n^{(s)}\right)$ is Cauchy, thus the second term on the right hand side converges to zero and since $[\alpha_n]$ is Cauchy, so does the first term. The latter holds since we must have that $\left|a_t^{(n)} - a_t^{(m)}\right|$ converges to zero as n, m, t tend to ∞. Therefore, α is an element of $\widehat{K}$. Furthermore, $[\alpha_n]$ converges to α. To see this, note that

$$\lim |\alpha_n - \alpha_m| = \lim \lim \left|a_m^{(n)} - a_m^{(m)}\right| = 0$$

hence $[\alpha_n]$ has a limit in $\widehat{K}$, implying that $\widehat{K}$ is complete.

Corollary 3.20. *The completion $(\widehat{K}, |\cdot|)$ of $(K, |\cdot|)$ is unique up to isomorphisms preserving the valuation on K.*

Proof. See Corollary 2.3 in [3]. □

3.3 p-adic numbers and p-adic integers

Let p be a prime number. Every nonzero rational number $x \in \mathbb{Q}$ can be uniquely written in the form

$$x = p^n \cdot \frac{a}{b}$$

where $a, b \in \mathbb{Z}$ are not divisible by p, and $n \in \mathbb{Z}$. The exponent n is called the *p-adic valuation* of x, denoted $v_p(x) := n$.

The *p-adic absolute value* is then defined by

$$|x|_p := p^{-v_p(x)}, \quad |0|_p := 0.$$

This defines a non-archimedean absolute value on $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ yields the field of *p-adic numbers*, denoted by $\mathbb{Q}_p$.

Definition 3.21. *The p-*adic integers *are defined as the valuation ring*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\} = \{x \in \mathbb{Q}_p : v_p(x) \geqslant 0\},$$

that is, $\mathbb{Z}_p$ is the valuation ring of $\mathbb{Q}_p$.

Proposition 3.22. *The ring of p-adic integers have maximal ideal (p), and the residue field is $\mathbb{F}_p$.*

Proof. First, we show that the non-zero ideals of $\mathbb{Z}_p$ are precisely $p^n\mathbb{Z}_p$ for $n \geqslant 0$. Let $0 \neq I \subseteq \mathbb{Z}_p$ be an ideal and choose $x \in I$ so that $|x|_p$ is maximal. Note that it is indeed possible to choose such an x since the possible values of the absolute value are discrete and bounded from above. Consider, additionally some $y \in I$. By maximality of x we have

$$|y|_p \leqslant |x|_p \Rightarrow |yx^{-1}|_p \leqslant 1$$

and hence $xy^{-1} \in \mathbb{Z}_p$. It follows that $y = (yx^{-1})x \in x\mathbb{Z}_p$, implying that $I \subseteq \mathbb{Z}_p$. The inclusion $x\mathbb{Z}_p \subseteq I$ is clear. Therefore $I = x\mathbb{Z}_p$.

Denote $x = p^n\dfrac{a}{b}$. We have that $\dfrac{a}{b}$ is invertible in $\mathbb{Z}_p$ hence $x\mathbb{Z}_p = p^n\mathbb{Z}_p$.

Next, we claim that

$$\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

To show this, consider the map

$$\begin{aligned} f_n : \mathbb{Z} &\to \mathbb{Z}_p/p^n\mathbb{Z}_p \\ x &\mapsto \bar{x}, \end{aligned}$$

i.e., $f_n = \pi \circ \iota$ where π and ι are the canonical and inclusion maps respectively. This map is a surjective ring homomorphism (Corollary 4.2.5 in [2]) and

$$p^n\mathbb{Z}_p = \{x : |x|_p \leqslant p^{-n}\}$$

so we must have

$$\ker f_n = \{x \in \mathbb{Z} : |x|_p \leqslant p^{-n}\} = p^n\mathbb{Z},$$

hence by the *First Isomorphism Theorem* we have

$$\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

Now, note that $\mathbb{Z}/p^n\mathbb{Z}$ is a field if and only if $p = 1$, and consequently from above, so is $\mathbb{Z}_p/p\mathbb{Z}_p$ hence (p) is the unique maximal ideal of $\mathbb{Z}_p$. □

A very important result that will help us in determining squares in $\mathbb{Q}_p$, or more importantly non-squares, is the following theorem.

Theorem 3.23 (Hensel's Lemma, version 1)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ such that*

$$\begin{aligned} f(a) &\equiv 0 \pmod{p}, \\ f'(a) &\not\equiv 0 \pmod{p}. \end{aligned}$$

Then, there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ in $\mathbb{Z}_p$ and $\alpha \equiv a \pmod{p}$.

Proof. We start by proving that for all $n \geqslant 1$, there exists an $a_n \in \mathbb{Z}_p$ such that

$$f(a_n) \equiv 0 \pmod{p^n} \qquad \text{and} \qquad a_n \equiv a \pmod{p}$$

using induction. The case $n = 1$ follows immediately by taking $a_1 = a$. Assume now that the statement holds for $n \geqslant 1$. Then, we need to find some $a_{n+1} \in \mathbb{Z}_p$ such that

$$f(a_{n+1}) \equiv 0 \pmod{p^{n+1}} \qquad \text{and} \qquad a_{n+1} \equiv a \pmod{p}.$$

By the induction hypothesis, there exists some a_n such that it is a root of $f \mod p^n$ and $a_n \equiv a \pmod p$, therefore, we are looking for $a_{n+1} \in \mathbb{Z}_p$ such that $a_{n+1} \equiv a_n \pmod{p^n}$ and $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$. To this end, we write

$$a_{n+1} \equiv a_n + p^n t_n$$

for some $t_n \in \mathbb{Z}_p$ that we shall find later. We need to show that for our chosen t_n, we can make

$$f(a_n + p^n t_n) \equiv 0 \pmod{p^{n+1}}.$$

Let $x, y \in \mathbb{Z}_p[x, y]$ and write $f(x) = \sum_{i=0}^{d} c_i x^i$, with $c_i \in \mathbb{Z}_p$ for all i. Then

$$\begin{aligned} f(x+y) &= \sum_{i=0}^{d} c_i (x+y)^i \\ &= c_0 + \sum_{i=1}^{d} (c_i(x^i + ix^{i-1}y) + g_i(x,y)y^2) \end{aligned}$$

where the second equality was obtained by separating the terms with factors of y^2 in the binomial expansion, and $g_i(x, y) \in \mathbb{Z}_p[x, y]$. Rearranging then gives

$$\begin{aligned} f(x+y) &= \sum_{i=0}^{d} x^i + \sum_{i=1}^{d} ic_i x^{i-1} y + \sum_{i=1}^{d} c_i g_i(x,y) y^2 \\ &= f(x) + f'(x)y + g(x,y)y^2 \end{aligned}$$

where $g(x, y) = \sum_{i=1}^{d} c_i g_i(x, y) \in \mathbb{Z}_p[x, y]$. Thus, for all u and v in $\mathbb{Z}_p$, we have that $w := g(u, v) \in \mathbb{Z}_p$, so we have

$$f(u+v) = f(u) + f'(u)v + wv^2, \qquad \forall u, v \in \mathbb{Z}_p \text{ and } w = g(u,v).$$

Set $u = a_n$ and $y = p^n t_n$. This yields

$$\begin{aligned} f(a_n + p^n t_n) &= f(a_n) + f'(a_n)p^n t_n + z p^{2n} t_n^2 \\ &\equiv f(a_n) + f'(a_n)p^n t_n \pmod{p^{n+1}} \end{aligned}$$

since $2n \geqslant n+1$ and, hence, $p^{2n} \equiv 0 \pmod{p^{n+1}}$. Now, in $f'(a_n)p^n t_n \pmod{p^{n+1}}$, we only look at $f'(a_n)t_n$ modulo p, as there is already a factor of p^n in the term. Therefore, since we also have that $a_n \equiv a \pmod p$, we have

$$f'(a_n)t_n \equiv f'(a)t_n \pmod p$$

which gives

$$f'(a_n)p^n t_n \equiv f'(a)p^n t_n \pmod{p^{n+1}}.$$

As such, combining everything together yields

$$f(a_n + p^n t_n) \equiv 0 \pmod{p^{n+1}} \iff f(a_n) + f'(a)p^n t_n \equiv 0 \pmod{p^{n+1}}$$

and since $f(a_n) \equiv 0 \pmod{p^n}$ by assumption, $f(a_n)/p^n \in \mathbb{Z}_p$, and thus,

$$f'(a)t_n \equiv -f(a_n)/p^n \pmod p.$$

The above congruence has a solution for t_n as we assumed that $f'(a) \not\equiv 0 \pmod p$. With this choice of t_n, we are now able to let $a_{n+1} = a_n + p^n t_n$ so that $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$ and $a_{n+1} \equiv a_n \pmod{p^n}$, or in particular, $a_{n+1} \equiv a \pmod p$.

We have constructed a sequence $(a_n)_{n>0} \in \mathbb{Z}_p$ such that

$$f(a_n) \equiv 0 \pmod{p^n} \qquad \text{and} \qquad a_{n+1} \equiv a_n \pmod{p^n}, \qquad \forall n > 0.$$

The second condition implies that $a_{n+1} - a_n \equiv 0 \pmod{p^n}$, and hence, $|a_{n+1} - a_n|_p \leqslant n$, in particular, $(a_n)_{n>0}$ is Cauchy in $\mathbb{Z}_p$. Let α be the limit of this sequence in $\mathbb{Z}_p$. We aim to show that

$$f(\alpha) = 0 \qquad \text{and} \qquad \alpha \equiv a \pmod{p}.$$

From $a_{n+1} \equiv a_n \pmod{p^n}$, for all n, we obtain

$$a_m \equiv a_n \pmod{p^n}$$

for all m and n such that $m > n$. Thus, by letting $m \to \infty$, there exists an $\alpha \in \mathbb{Z}_p$ such that

$$\alpha \equiv a_n \pmod{p^n}$$

and at $n = 1$, we obtain precisely $\alpha \equiv 1 \pmod{p}$. Now, for general n we have

$$f(\alpha) \equiv f(a_n) \equiv 0 \pmod{p^n}$$

hence

$$|f(\alpha)|_p \leqslant \frac{1}{p^n}.$$

Since the above is true for all n, as $n \to \infty$

$$|f(\alpha)|_p \leqslant 0 \iff f(\alpha) = 0.$$

We are now left to prove uniqueness. Suppose there exists some $\beta \in \mathbb{Z}_p$ such that $f(\beta) = 0$ and $\beta \equiv a \pmod{p}$. In order to show that $\alpha = \beta$, we will show inductively that $\beta \equiv \alpha \pmod{p^n}$, for all n. The case $n = 1$ is clear since both α and β are congruent to a modulo p. Assume that $\beta \equiv \alpha \pmod{p^n}$, and show for $n+1$. Then

$$\beta = a_n + p^n \gamma_n, \qquad \gamma_n \in \mathbb{Z}_p.$$

Then, from a computation entirely similar to the one above we have

$$f(\beta) = f(\alpha + p^n \gamma_n) \equiv f(\alpha) + f'(\alpha) p^n \gamma_n \pmod{p^{n+1}}.$$

Since both α and β solve $f(x) = 0$, we have

$$f'(\alpha) p^n \gamma_n \equiv 0 \pmod{p^{n+1}}$$

and since p^n is already a factor on the left hand side above,

$$f'(\alpha) \gamma_n \equiv 0 \pmod{p}.$$

But $f'(\alpha) \equiv f'(a) \not\equiv 0 \pmod{p}$ hence,

$$\gamma_n \equiv 0 \pmod{p}$$

which implies that

$$\beta \equiv \alpha \pmod{p^{n+1}}.$$

Thus, we have $\beta - \alpha \equiv 0 \pmod{p^n}$ for all n, that is,

$$|\alpha - \beta|_p \leqslant \frac{1}{p^n}$$

and as $n \to \infty$, we obtain precisely that $\alpha = \beta$. □

Then, with Hensel's Lemma in hand, we can determine how squares actually look like in $\mathbb{Q}_p$.

Theorem 3.24. *An element $\alpha \in \mathbb{Q}_p^\times$, where $p \neq 2$ is a square in $\mathbb{Q}_p$ if and only if $v_p(\alpha)$ is even and u is a quadratic residue in $\mathbb{F}_p$.*

Proof. Note that any element $\alpha \in \mathbb{Q}_p$ can be written as

$$\alpha = p^{v_p(\alpha)}u, \qquad u \in \mathbb{Z}_p^\times.$$

Thus, we first show that $u \in \mathbb{Z}_p^\times$ is a square in $\mathbb{Q}_p$ if and only if u is a square in $\mathbb{F}_p$.

($\Leftarrow$) : Assume that u is a quadratic residue modulo p. We have, essentially by definition, that $u \in \mathbb{Z}_p^\times$ is a square if and only if the polynomial

$$f(x) = x^2 - u$$

splits in $\mathbb{Z}_p[x]$. That is, there exists an a such that

$$f(a) \equiv 0 \pmod{p}.$$

Moreover, a cannot be a a double root of $f(x) \mod p$ since $f'(x) = 2x$ and $p \neq 2$, so $f'(a) \not\equiv 0 \pmod{p}$. Then, by Hensel's Lemma (3.23), there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ in $\mathbb{Z}_p$ and $\alpha \equiv a \pmod{p}$.

($\Rightarrow$) : Conversely, assume that $u = a^2$ in $\mathbb{Q}_p$. Then, since $u \in \mathbb{Z}_p^\times$, we have $v_p(u) = 0$, and hence, $v_p(a) = 0$, implying that $a \in \mathbb{Z}_p^\times$. Now, we saw in Proposition 3.22, that $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Since the reduction map is a ring homomorphism, it respects squaring, so we are done.

We can now extend this result to $\mathbb{Q}_p$. It is clear that if $v_p(x)$ is even and $u = v^2 \in \mathbb{Z}_p$, we can write x as

$$\alpha = \left(p^{v_p(\alpha)/2}v\right)^2$$

where $p^{v_p(\alpha)/2}v \in \mathbb{Q}_p^\times$.

If α is a square, then each factor of α is a square. That is, we need $p^{v_p(\alpha)}$ and $u \in \mathbb{Z}_p^\times$ to be squares. The former implies that $v_p(\alpha)$ must be even as its only nontrivial divisor is p, and the latter implies that u must be a square in $\mathbb{F}_p$. This proves the theorem. □

Squares in $\mathbb{Q}_2$ are a bit more complicated. The following is another version of Hensel's Lemma, which we will require in the characterization of squares in the 2-adic field.

Theorem 3.25 (Hensel's Lemma, version 2)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ such that*

$$|f(a)|_p < |f(a)|_p^2.$$

Then, there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ in $\mathbb{Z}_p$ and $|\alpha - a|_p < |f'(\alpha)|$. Moreover,

(i) $|\alpha - a|_p = |f(a)/f'(a)|_p < |f'(a)|_p$;

(ii) $|f'(\alpha)|_p = |f'(a)|_p$

Proof. A general version of this result is proven in Chapter 2, Section 1.5 of [9], and the specific form stated here follows immediately by taking $K = \mathbb{Q}_p$ and $A = \mathbb{Z}_p$. □

Theorem 3.26. *Let $\alpha \in \mathbb{Q}_2^\times$. Then $\alpha = p^{v_2(\alpha)}u$, with $u \in \mathbb{Z}_2^\times$ is a square in $\mathbb{Q}_2$ if and only if $v_2(\alpha)$ is even and $u \equiv 1 \pmod{8\mathbb{Z}_2}$.*

Proof. We first show that $u \in \mathbb{Z}_2^\times$ is a square if and only if $u \equiv 1 \pmod{8\mathbb{Z}_2}$.

($\Rightarrow$) : Assume that $u = a^2$ in $\mathbb{Q}_2$. Then, $v_2(a^2) = 0$ and hence, $v_2(a) = 0$, i.e., $a \in \mathbb{Z}_2^\times$. Furthermore, from Example 3.22 we know

$$\mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}.$$

The units in $\mathbb{Z}/8\mathbb{Z}$ are 1, 3, 5 and 7 and all of their squares are congruent to 1 modulo 8. Therefore

$$u \equiv a^2 \equiv 1 \pmod{8\mathbb{Z}_2}.$$

($\Leftarrow$) : Conversely, assume that $u \equiv 1 \pmod{8\mathbb{Z}_2}$. We have that u is a square in $\mathbb{Q}_2$ if and only if $f(x) = x^2 - u$ splits in $\mathbb{Q}_2$. Thus consider the polynomial $f(x)$. We shall use $a = 1$ in Hensel's Lemma (3.25). Indeed, we have that

$$|f(1)|_2 = |1 - u|_2 \leqslant \frac{1}{8}$$

since $u \equiv 1 \pmod{8\mathbb{Z}_2}$, and

$$|f'(1)|_2 = |2|_2 = \frac{1}{2},$$

hence $|f(1)|_2 < |f'(1)|_p^2$. Then, there exists a unique α such that $f(\alpha) = 0$ in $\mathbb{Z}_2$, that is, u is a square in $\mathbb{Z}_2$.

Now, similarly to the proof of Theorem 3.24, we can extend this result to $\mathbb{Q}_p^\times$, by noting that for all $\alpha \in \mathbb{Q}_2$ we can write

$$\alpha = p^{v_2(\alpha)}u, \qquad u \in \mathbb{Z}_2^\times,$$

then, by a completely analogous argument as in Theorem 3.24, we are done. □

3.4 Local fields

Definition 3.27 (Local field)**.** *A* local field *is a field that is complete with respect to a discrete valuation and has a finite residue field.*

Example 3.28. *The field $\mathbb{Q}_p$ is a local field: it is complete with respect to the p-adic valuation, and its residue field $\mathbb{F}_p$ is finite.*

Remark 3.29. *In the local setting, we refer to the valuation ring $O_K = \{x \in K : v(x) \geqslant 0\}$ as the* ring of integers *of K, as we saw in Proposition 3.16 that O_K is indeed integrally closed.*

3.4.1 Extensions and ramification

In this section, we return to the concept of ramification, but now we look at it through a local lens. In what follows, we shall consider some finite extension of local fields L/K equipped with the discrete valuation v_L and v_K. We also let O_L and O_K be the rings of integers of L and K respectively, $\mathfrak{m}_L$ and $\mathfrak{m}_K$, their maximal ideals, π_L and π_K their respective uniformizers, and ℓ and k their residue fields.

We revisit the notion of ramification in the local setting, where it is described in terms of valuation.

Definition 3.30. *The integer*

$$e_{L/K} = v_L(\pi_K)$$

is the ramification index *of* L/K.

We say that L/K is ramified if $e_{L/K} > 1$, and moreover, as in the number fields case, we define:

Definition 3.31 (Unramified extension)**.** *The extension L/K is unramified if $e_{L/K} = 1$.*

Definition 3.32 (Totally ramified extension)**.** *We say that L/K is totally ramified if $e_{L/K} = [L : K]$*

The definitions of trace, norm and discriminant for finite extensions of local fields mirror those given in Section 2 for number fields. Given an extension L/K of local fields, the trace and norm of an element $\alpha \in L$ are defined via the K-linear map $x \mapsto \alpha x$, just as in the global case. Moreover, these maps satisfy the same properties as over number fields: the norm of α is the product of all its K-embeddings into the algebraic closure of K, and the trace is the corresponding sum (see Proposition 2.9). Likewise, the discriminant of a basis of L/K is defined using the matrix of embeddings applied to the basis (Definition 2.10). The discriminant of L/K is the ideal generated by the discriminant of integral bases, which, in the local setting coincide with the bases of the discrete valuation ring O_L (Proposition 3.16).

Proposition 3.33. *Let L/K be a finite extension of local fields. Then, the unique extension of the valuation on K to L is given by the formula*

$$v_L(y) = \frac{1}{[L : K]} v_K(N_{L/K}(y)) \tag{1}$$

for all y in L.

Proof. See Corollary 3.4 in [3] where this result is given in the equivalent form using absolute values:

$$|y|_L = |N_{L/K}(y)|_K^{1/[L:K]}.$$

The two formulations are equivalent via the identity

$$|x|_K = \pi^{-v_K(x)}$$

where π is a uniformizer of K. □

Remark 3.34. *Valuations on local fields are normalized so that their image is $\mathbb{Z}$ and a uniformizer has valuation* 1*. When computing valuations via the formula above the result may appear as a rational number. This indicates that the valuation is not normalized, and one must rescale appropriately to obtain a genuine discrete valuation.*

3.4.2 Ramified and unramified quadratic extensions of $\mathbb{Q}_p$

Quadratic extensions of $\mathbb{Q}_p$, where $p > 2$

Let $L = \mathbb{Q}_p(\sqrt{d})$, where $d \in \mathbb{Z}_p$ is squarefree and $p > 2$. We study the ring of integers $\mathcal{O}_L$, the extended valuation v_L, and determine whether the extension $L/\mathbb{Q}_p$ is ramified or unramified. We distinguish two cases, depending on whether $d = u$ or $d = pu$ for some unit $u \in \mathbb{Z}_p^\times$.

General setup. The embeddings of L into $\overline{\mathbb{Q}}_p$ are given by

$$\sigma_1(\sqrt{d}) = \sqrt{d}, \qquad \sigma_2(\sqrt{d}) = -\sqrt{d}.$$

As d is squarefree and $x^2 - d$ is irreducible over $\mathbb{Q}_p$, we have that $\{1, \sqrt{d}\}$ is a $\mathbb{Q}_p$-basis of L. Every element $x \in L$ can be written uniquely as

$$x = a + b\sqrt{d}, \qquad \text{with } a, b \in \mathbb{Q}_p.$$

We now show that the ring of integers $\mathcal{O}_L$ is precisely $\mathbb{Z}_p[\sqrt{d}]$.

Let $x = a + b\sqrt{d} \in \mathcal{O}_L$. Then x is integral over $\mathbb{Z}_p$, so its minimal polynomial

$$x^2 - 2ax + a^2 - b^2 d$$

must have coefficients in $\mathbb{Z}_p$. Since $p > 2$, we have $v_p(2a) = v_p(a)$, so $a \in \mathbb{Z}_p$. Also, $a^2 - b^2 d \in \mathbb{Z}_p$ implies that $b^2 d \in \mathbb{Z}_p$.

From Theorem 3.24, we know that $\alpha = p^{v_p(\alpha)}u \in \mathbb{Q}_p^\times$ is a square in $\mathbb{Q}_p$ if and only if $v_p(\alpha)$ is even and u is a quadratic residue modulo p. So we either have $d = pu$, with $u \in \mathbb{Z}_p^\times$, or $d = u \in \mathbb{Z}_p^\times$ and u not a quadratic residue modulo p. If $d = pu$ we have

$$v_p(b^2 pu) \geqslant 0 \iff 2v_p(b) + 1 \geqslant 0 \iff v_p(b) \geqslant -\frac{1}{2}$$

and since the image of v_p is $\mathbb{Z}$, we have $v_p(b) \geqslant 0$, i.e., $b \in \mathbb{Z}_p$. Similarly, if $d = u$,

$$v_p(b^2 d) \geqslant 0 \iff 2v_p(b) + 0 \geqslant 0 \iff v_p(b) \geqslant 0$$

Hence $b \in \mathbb{Z}_p$ in both cases. Then

$$x = a + b\sqrt{d} \in \mathbb{Z}_p[\sqrt{d}],$$

so $\mathcal{O}_L = \mathbb{Z}_p[\sqrt{d}]$, as the reverse inclusion is clear.

Now, in order to study the possible ramifications of L, we distinguish between the two cases, the first one, $d = u \in \mathbb{Z}_p^\times$ where u is not a quadratic residue modulo p, which yields a unramified extension, and the second, $d = pu$, with $u \in \mathbb{Z}_p^\times$ which gives a (totally) ramified extension.

I. Unramified extension.
Let $d = u$, where $u \in \mathbb{Z}_p^\times$ is not a square modulo p, i.e., $u \notin (\mathbb{F}_p^\times)^2$.

From Proposition 3.33, the valuation of $\sqrt{u} \in L$ is

$$v_L(\sqrt{u}) = \frac{1}{2}v_p(N(\sqrt{u})) = \frac{1}{2}v_p(-u) = 0.$$

Define $\pi_L := p\sqrt{u}$. Then:

$$v_L(p\sqrt{u}) = \frac{1}{2}v_p(N(p\sqrt{u})) = \frac{1}{2}v_p(-p^2u) = 1.$$

So π_L is a uniformizer in $\mathcal{O}_L$. Since $v_L(p) = 1$, the ramification index is

$$e_{L/\mathbb{Q}_p} = v_L(p) = 1,$$

and the extension is unramified. The residue field is unchanged, i.e., $\mathbb{F}_p$.

We compute the discriminant with respect to the basis $\{1, \sqrt{u}\}$:

$$\Delta_{L/\mathbb{Q}_p}(1, \sqrt{u}) = \begin{vmatrix} 1 & \sqrt{u} \\ 1 & -\sqrt{u} \end{vmatrix}^2 = (-2\sqrt{u})^2 = 4u,$$

so the discriminant ideal $\Delta_{L/\mathbb{Q}_p}$ is generated by $4u$, and $v_p(\Delta_{L/\mathbb{Q}_p}) = 0$.

II. Ramified extension.
Let $d = pu$, where $u \in \mathbb{Z}_p^\times$. We show that $L/\mathbb{Q}_p$ is totally ramified and compute the discriminant.

We begin by showing that the value group of L is $\frac{1}{2}\mathbb{Z}$, that is, the valuation on L is originally unnormalized with the formula in Proposition 3.33. Let $x = a + b\sqrt{pu} \in L^\times$, then

$$N(x) = a^2 - b^2pu.$$

By Proposition 3.33, we have

$$v_L(N(x)) = \frac{1}{2}v_p(N(x)) \in \frac{1}{2}\mathbb{Z}$$

hence $v_L(L^\times) \subseteq \frac{1}{2}\mathbb{Z}$ Now, let $y = \frac{n}{2} \in \mathbb{Z}$ and consider $\sqrt{pu}^n \in L^\times$. We have

$$\begin{aligned} v_L(\sqrt{pu}^n) &= \frac{1}{2}v_p(N(\sqrt{pu}) \\ &= \frac{1}{2}v_p(\sigma_1(\sqrt{pu})^n\sigma_2(\sqrt{pu})^n) \\ &= \frac{1}{2}v_p(\sqrt{pu}^n(-\sqrt{pu})^n) \\ &= \frac{1}{2}v_p(\sqrt{pu}^{2n}) \\ &= \frac{1}{2}v_p(pu^n) \\ &= \frac{n}{2}, \end{aligned}$$

hence for all $y \in \frac{1}{2}\mathbb{Z}$, there exists some $x \in L^\times$ such that $v_L(x) = y$, that is, $v_p(L^\times) = \frac{1}{2}\mathbb{Z}$. Hence, $v_L(L^\times) = \frac{1}{2}\mathbb{Z}$. Since the value group of a discrete valuation must be $\mathbb{Z}$, we normalize v_L by setting $v_L^{\text{norm}} := 2v_L$. Then

$$v_L^{\text{norm}}(\sqrt{pu}) = v_p(N(\sqrt{pu})) = v_p(pu) = 1,$$

so $\sqrt{pu}$ is a uniformizer. Also,

$$v_L^{\text{norm}}(pu) = 2v_L(\sqrt{pu}^2) = 2,$$

and we conclude $e_{L/\mathbb{Q}_p} = 2$, so L is totally ramified.

Finally, we compute the discriminant:

$$\Delta(1, \sqrt{pu}) = \begin{vmatrix} 1 & \sqrt{pu} \\ 1 & -\sqrt{pu} \end{vmatrix}^2 = (-2\sqrt{pu})^2 = 4pu,$$

so the discriminant ideal is generated by $4pu$, and $v_p(\Delta_{L/\mathbb{Q}_p}) = 1$.

Quadratic extensions of $\mathbb{Q}_2$

Let us now consider a quadratic extension of $\mathbb{Q}_2$, i.e., $L := \mathbb{Q}_2(\sqrt{d})$, with $d \in \mathbb{Z}_2$ squarefree. From Theorem 3.26, an element $\alpha = 2^{v_2(\alpha)}u$, with $u \in \mathbb{Z}_2^\times$, of $\mathbb{Q}_2^\times$ is a square in $\mathbb{Q}_2$ if and only if $v_2(\alpha)$ is even and $u \equiv 1 \pmod{8\mathbb{Z}_2}$. Therefore, we can only have that $d = pu$ with $u \in \mathbb{Z}_2^\times$, or $d = u \in \mathbb{Z}_2^\times$ such that $u \not\equiv 1 \pmod{8\mathbb{Z}_2}$.

We start by finding the ring of integers $\mathcal{O}_L$ of L. Let $\alpha \in \mathcal{O}_L \subseteq L$. Then, since a $\mathbb{Q}_2$-basis for L is given by $\{1, \sqrt{d}\}$, we can write

$$\alpha = \frac{a + b\sqrt{d}}{c}, \qquad a, b, c \in \mathbb{Z}_2$$

and we can assume without loss of generality that $\gcd(a, b, c) = 1$ (note that the gcd is well defined as we are in a unique factorization domain). Then, the minimal polynomial of α is given by

$$x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}_2[x].$$

Since all coefficients must be in $\mathbb{Z}_2$, if $\gcd(a, b) = m$, from the constant term, it must be that $\gcd(c, m) = m$ since d is squarefree, thus we need $\gcd(a, b) = 1$. From the linear coefficient we have

$$v_2\left(\frac{2a}{c}\right) \geqslant 0 \iff v_2(a) \geqslant 1 - v_2(c)$$

hence we require that $v_2(c) = 0$ or $v_2(c) = 1$. Suppose that $v_2(c) = 1$. If $v_2(a) > 0$, then $\gcd(a, c) = c$, but this also implies that $\gcd(b^2 d, c^2) = c^2$, and since d is squarefree, that $\gcd(b, c) = c$, a contradiction. Hence, $v_2(a) = 0$. We need that

$$v_2(a^2 - b^2 d) \geqslant 2v_2(c) = 4,$$

or, in other words,

$$a^2 - b^2 d \equiv 0 \pmod{4\mathbb{Z}_2} \iff a^2 \equiv b^2 d \pmod{4\mathbb{Z}_2}.$$

Now, we know that $\mathbb{Z}_2/4\mathbb{Z}_2 \cong \mathbb{Z}/4\mathbb{Z}$ from the proof of Proposition 3.22, and in $\mathbb{Z}/4\mathbb{Z}$ all quadratic residues are congruent to either 1 or 0 modulo 4. Thus, since $v_2(a) = 0$, we must have $a^2 \equiv 1 \pmod{4\mathbb{Z}_2}$ so,

$$b^2 d \equiv 1 \pmod{4\mathbb{Z}_2}$$

and this implies that $b^2 \equiv 1 \pmod{4\mathbb{Z}_2}$. Therefore,

$$d \equiv 1 \pmod{4\mathbb{Z}_2}.$$

If $d = 2u$, this is clearly impossible, hence we need $d = u$. Note that in this case, if $u \equiv 1 \pmod{4\mathbb{Z}_2}$, we obtain that $u \equiv 1 \pmod{8\mathbb{Z}_2}$ or $u \equiv 5 \pmod{8\mathbb{Z}_2}$. The former is excluded by assumption since we assumed d is squarefree, i.e., $d = u \not\equiv 1 \pmod{8\mathbb{Z}_2}$ hence,

$$u \equiv 5 \pmod{8\mathbb{Z}_2}.$$

Therefore, in this case, a basis for O_L is

$$\left\{1,\ \frac{1+\sqrt{u}}{2}\right\}.$$

Assume now that $v_2(c) = 0$. Then we can write

$$\alpha = a + b\sqrt{d}, \qquad a,\, b \in \mathbb{Z}_2$$

and hence, an integral basis in the remaining cases is given by

$$\{1,\ \sqrt{d}\}.$$

Putting everything together, we obtain

$$O_L = \begin{cases} \mathbb{Z}_2[\sqrt{2u}], & \text{if } d = pu,\ u \in \mathbb{Z}_2^\times \\ \mathbb{Z}_2[\sqrt{u}], & \text{if } d = u \not\equiv 1 \pmod{8\mathbb{Z}_2} \text{ and } u \not\equiv 5 \pmod{8\mathbb{Z}_2}, \\ \mathbb{Z}_2\left[\frac{1+\sqrt{u}}{2}\right], & \text{if } d = u \in \mathbb{Z}_2^\times \text{ and } u \equiv 5 \pmod{8\mathbb{Z}_2}. \end{cases}$$

Having the above, we are now able to study the ramification of quadratic extensions of $\mathbb{Q}_2$. Recall that Theorem 2.15 in Section 2 states that a prime p ramifies in some number field extension if and only if it divides the discriminant of the extension. For local fields, there is an analogous criterion: a finite extension L/K is ramified if and only if the valuation $v_K(\Delta_{L/K})$ of the discriminant is strictly positive, that is,

$$v_K(\Delta_{L/K}) > 0 \quad \Longleftrightarrow \quad L/K \text{ is ramified.}$$

Therefore, we can compute the ramifications in $L = \mathbb{Q}_2(\sqrt{d})/\mathbb{Q}_2$ by making use of the discriminant. We shall use the discriminant formula in Definition 2.10, and note that the embeddings into $\bar{\mathbb{Q}}_2$ are the same as above, for $p > 2$. To this end, we consider three cases:

I. $d = 2u$, $u \in \mathbb{Z}_2$.
Here we have $O_L = \mathbb{Z}_2[\sqrt{2u}]$ and so

$$\Delta_{L/\mathbb{Q}_2}(1,\ \sqrt{2u}) = \begin{vmatrix} 1 & \sqrt{2u} \\ 1 & -\sqrt{2u} \end{vmatrix}^2 = (-2\sqrt{2u})^2 = 8u,$$

hence $\Delta_{L/\mathbb{Q}_2} = (8u)$ and $v_2(\Delta_{L/\mathbb{Q}_2}) = 3$, in other words L is ramified.

II. $d = u \in \mathbb{Z}_2^\times$, $u \not\equiv 1 \pmod{8\mathbb{Z}_2}$ and $u \not\equiv 5 \pmod{8\mathbb{Z}_2}$.
The ring of integers of L is $O_L = \mathbb{Z}_2[\sqrt{u}]$. Then

$$\Delta_{L/\mathbb{Q}_2}(1,\ \sqrt{u}) = \begin{vmatrix} 1 & \sqrt{u} \\ 1 & -\sqrt{u} \end{vmatrix}^2 = (-2\sqrt{u})^2 = 4u,$$

that is, $\Delta_{L/\mathbb{Q}_2} = (4u)$ and $v_2(\Delta_{L/\mathbb{Q}_2}) = 2$, hence we have again a ramified extension.

III. $d = u \in \mathbb{Z}_2^\times$, $u \equiv 5 \pmod{8\mathbb{Z}_2}$.
This case gives

$$O_L = \mathbb{Z}_2\left[\frac{1+\sqrt{u}}{2}\right]$$

hence

$$\Delta_{L/\mathbb{Q}_2}\left(1,\ \frac{1+\sqrt{u}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{u}}{2} \\ 1 & \frac{1-\sqrt{u}}{2} \end{vmatrix}^2 = \left(-\frac{2\sqrt{u}}{2}\right)^2 = u.$$

From here we obtain $\Delta_{L/\mathbb{Q}_2} = (u)$ and $v_2(\Delta_{L/\mathbb{Q}_2}) = 0$, in other words, an unramified extension.

4 Elliptic Curves

The central topics of this paper gravitate around *elliptic curves*. To rigorously define them, we begin by introducing basic notions about curves, both affine and projective. In particular, we focus on projective curves defined by homogeneous polynomials in the projective plane, and discuss the transition between projective and affine descriptions. This allows us to define smoothness, classify singularities (nodes and cusps), and formally introduce elliptic curves.

Definition 4.1 (Projective curve)**.** *Let K be a field. A* projective curve *over K is a subset of the projective sapce $\mathbb{P}^2(K)$ defined by a single homogeneous polynomial $F(X,Y,Z) \in K[X,Y,Z]$ of degree at least 1. That is, the projective curve C is the set of all points $[X:Y:Z] \in \mathbb{P}^2(K)$ such that*

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

Note that given a projective curve defined by a homogeneous polynomial $F(X,Y,Z)$, we can obtain an affine equation by using the non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$, whenever $Z \neq 0$. This yields a planar (affine) curve in $\mathbb{A}^2(K)$ defined by a non-homogeneous polynomial $f(x,y)$ and some additional point at infinity where $Z = 0$.

Example 4.2. *Consider the projective curve defined by the Weierstrass equation*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

over $\mathbb{P}^2(K)$, where K is a field.

Whenever $Z \neq 0$, through the non-homogeneous coordinate change $x = X/Z$ and $y = Y/Z$, we obtain:

$$y^2Z^3 + a_1xyZ^3 + a_3yZ^3 = x^3Z^3 + a_2x^2Z^3 + a_4xZ^3 + a_6Z^3$$

which is equivalent to

$$f(x,y) =: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Now, if $Z = 0$ this coordinate change gives a point at infinity. Substituting $Z = 0$ into the homogeneous equation gives

$$Y^2 \cdot 0 + a_1XY \cdot 0 + a_3Y \cdot 0 = X^3 + a_2X^2 \cdot 0 + a_4X \cdot 0 + a_6 \cdot 0 \iff X^3 = 0.$$

Thus, the solution at infinity is $[X:Y:Z] = [0:Y:0] = [0:1:0]$. Therefore, we can write the Weierstrass equation as a planar curve $f(x,y)$ together with a distinguished point at infinity $O = [0:1:0]$.

Definition 4.3 (Smooth curve)**.** *Let $f(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$ be a polynomial over a field K, and let $P = (a_1,\ldots,a_n) \in K^n$ be a point such that $f(P) = 0$. We say that the point P is* smooth *(or* nonsingular*) on the curve defined by f if there exists some $i \in \{1,\ldots,n\}$ such that*

$$\frac{\partial f}{\partial X_i}(P) \neq 0$$

We say that the curve C, defined as the set of zeros of the polynomial f is smooth *if every point on it is smooth.*

In the case that

$$\frac{\partial f}{\partial X_i}(P) = 0$$

for all $i \in \{1, \ldots, n\}$, the point P is said to be singular, and if $P \in C$ is singular, then the curve is singular.

Consider now some point $P = (x_0, y_0)$ satisfying a Weierstrass equation:

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

and suppose that P is singular on $f(x,y) = 0$. Then,

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0,$$

hence there exists $\alpha, \beta \in \bar{K}$ such that the second order Taylor expansion at P has the form

$$f(x,y) - f(x_0,y_0) = ((y-y_0) - \alpha(x-x_0))(y-y_0) - \beta(x-x_0)) - (x-x_0)^3.$$

With the notation as above, we then define:

Definition 4.4 (Node and cusp)**.** *The singular point P is a node if $\alpha \neq \beta$. In this case the lines*

$$y - y_0 = \alpha(x - x_0) \quad \textit{and} \quad y - y_0 = \beta(x - x_0)$$

are the tangent lines at P.

Conversely, if $\alpha = \beta$, we call P a cusp, with tangent line given by

$$y - y_0 = \alpha(x - x_0).$$

To illustrate the two types of singularities that may arise on plane cubic curves, Figure 1 below shows two examples described by Weierstrass equations: a curve with a cusp and a curve with a node.

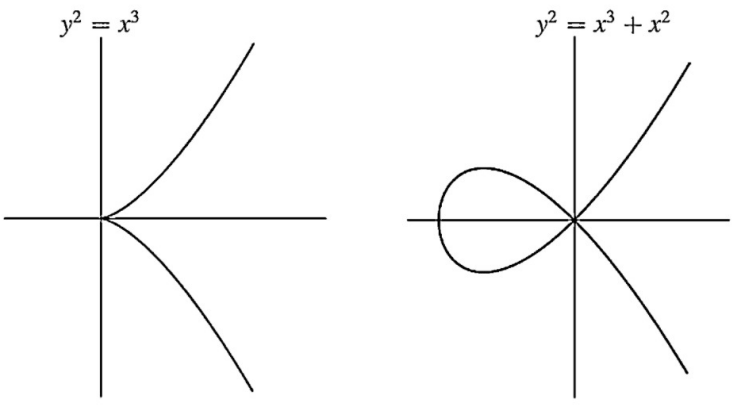

Figure 1: Singular curves: Cusp (left) and Node (right).

Definition 4.5 (Elliptic curve)**.** *An* elliptic curve *E over a field K is a smooth projective curve equipped with a distinguished point at infinity, and given by the set of solutions to a Weierstrass equation over K of the form:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2}$$

where $a_i \in K$ for all $i \in \{1, \ldots, 6\}$. The distinguished point at infinity is taken to be $O = [0 : 1 : 0]$.

Figure 2 provides three examples of elliptic curves, each illustrating different shapes depending on the coefficients in the Weierstrass equations describing them.

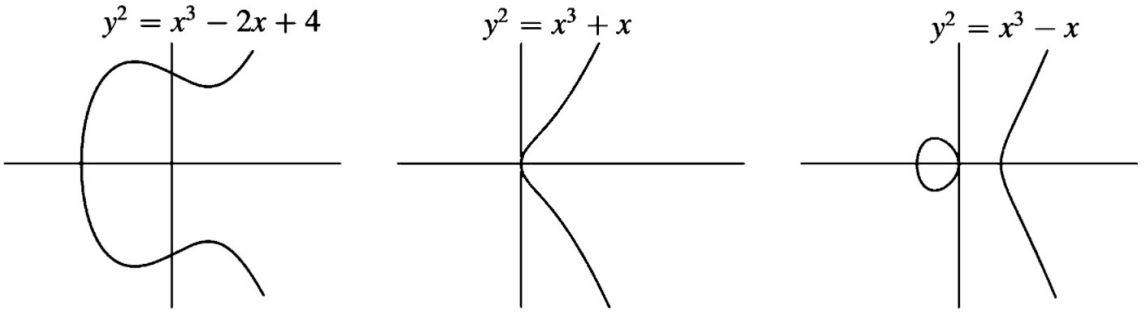

Figure 2: Three elliptic curves.

Claim 1: If $\mathrm{char}(K) \neq 2$, the equation can be simplified to:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{3}$$

where

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6,$$

by applying the substitution:

$$y \mapsto \frac{1}{2}(y - a_1x - a_3).$$

Proof. With the substitution above, we have:

$$\begin{aligned} y^2 &\mapsto \frac{1}{4}(y^2 + (a_1x)^2 + a_3^2 - 2a_1xy - 2a_3y + 2a_1a_3x); \\ a_1xy &\mapsto \frac{1}{2}(a_1xy - (a_1x)^2 - a_1a_3x); \\ a_3y &\mapsto \frac{1}{2}(a_3y - a_3a_1x - a_3^2). \end{aligned}$$

Then, by substituting the above into the equation for E, multiplying it by 4 and rearranging we have:

$$y^2 + (2a_1 - 2a_1)xy + (-2a_3 + 2a_3)y = 4x^3 + (2a_1^2 - a_1^2 + 4a_2)x^2 + (2a_1a_3 + 4a_4)x + (a_3^2 + 4a_6)$$

which, after simplification gives

$$y^2 = 4x^3 + (a_1^2 + 4a_2)x^2 + 2(2a_4 + a_1a_3)x + (a_3^2 + 4a_6)$$

hence we are done. □

Claim 2: If additionally $\mathrm{char}(K) \neq 3$, the curve can be transformed into the short Weierstrass form:

$$E : y^2 = x^3 - 27c_4x - 54c_6, \tag{4}$$

using the substitution:

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right),$$

where

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Proof. We compute the following:

$$\begin{aligned}
y^2 &\mapsto \frac{y^2}{108^2}; \\
4x^3 &\mapsto \frac{4}{36^3}(x^3 - 9b_2x^2 + 27b_2^2x - 27b_2^3); \\
b_2x^2 &\mapsto \frac{1}{36^2}(b_2x^2 - 6b_2^2x + 9b_2^3); \\
2b_4x &\mapsto \frac{1}{36}(2b_4x - 6b_2b_4).
\end{aligned}$$

Now, multiplying the new equation by 108^2 gives:

$$\begin{aligned}
108^2 \cdot y^2 &\mapsto y^2; \\
108^2 \cdot 4x^3 &\mapsto x^3 - 9b_2x^2 + 27b_2^2x - 27b_2^3; \\
108^2 \cdot b_2x^2 &\mapsto 9(b_2x^2 - 6b_2^2x + 9b_2^3); \\
108^2 \cdot 2b_4x &\mapsto 324(2b_4x - 6b_2b_4).
\end{aligned}$$

Then, the right hand side of the equation is given by

$$\begin{aligned}
&x^3 + (-9b_2 + 9b_2)x^2 + (27b_2^2 - 54b_2^2 + 648b_4)x + (-27b_2^3 + 81b_2^3 - 6 \cdot 324b_2b_4 + 108^2b_6) = \\
&x^3 - 27(b_2^2 - 24b_4)x - 54(-b_2^3 + 36b_2b_4 - 216b_6) = \\
&x^3 - 27c_4x - 54c_6
\end{aligned}$$

and the left hand side is precisely y^2. This finalizes the proof. □

Thus, by applying suitable coordinate changes, every elliptic curve over a field of characteristic not 2 or 3 can be written in the simplified form:

$$E : y^2 = x^3 + Ax + B,$$

where $A, B \in \overline{K}$.

Example 4.6. *Consider the elliptic curve $E/\mathbb{Q}$ given by the equation*

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 2$$

Since the characteristic of $\mathbb{Q}$ is 0, we can simplify this equation. First, compute

$$b_2 = 1^2 - 4 \cdot 1 = -3;$$

$$b_4 = -2 \cdot 5 + 1 \cdot 1 = -9;$$
$$b_6 = 1^2 + 4 \cdot 2 = 9;$$

and then, through

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

to obtain

$$c_4 = 3^2 + 24 \cdot 9 = 225;$$
$$c_6 = -3^3 + 36 \cdot 3 \cdot 9 - 216 \cdot 9 = -945$$

which gives the simplified equation for E:

$$y^2 = x^3 - 27 \cdot 225x + 54 \cdot 945.$$

We now introduce a few classical invariants associated to elliptic curves:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ \Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \\ j &= \frac{c_4^3}{\Delta}, \\ \omega &= \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y}. \end{aligned}$$

The Δ quantity is called the discriminant of the equation, j the $j-$invariant and ω the invariant differential.

Example 4.7. *Consider the elliptic curve $E/\mathbb{Q}$ given by the equation in Example 4.6:*

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 2.$$

Then we have

$$\begin{aligned} \Delta &= -3^2(1 \cdot 2 + 4 \cdot (-1) \cdot 2 + 1 \cdot 1 \cdot 5 - 1 \cdot 1^2 - 25) - 8 \cdot (-9)^3 - 27 \cdot 9^2 + 9 \cdot 3 \cdot 9 \cdot 9) \\ &= 6075 = 3^5 \cdot 5^2 \end{aligned}$$

and

$$j = \frac{225^3}{6075} = \frac{3^6 \cdot 5^6}{3^5 \cdot 5^2} = 3 \cdot 5^4.$$

In the simplified form $y^2 = x^3 + Ax + B$, valid when $\mathrm{char}(K) \neq 2, 3$, the discriminant and j-invariant become:

$$\Delta = -16(4A^3 + 27B^2), \qquad j = -1728 \cdot \frac{(4A)^3}{\Delta}.$$

We note that the Weierstrass equation of an elliptic curve is unique up to a change of variables of the form

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + su^2x' + t, \tag{5}$$

where $u, r, s, t \in \bar{K}$ with $u \neq 0$. For the proof, see Chapter III, Proposition 3.1. (b) in [11]. In the case we have a simplified equation of the form $y^2 = x^3 + Ax + B$, the only change of variables preserving this form of the equation is

$$x = u^2x' \qquad \text{and} \qquad y = u^3y'$$

where $u \in \bar{K}^\times$. Moreover, for the new curve with coefficients A' and B', and discriminant Δ' we have:

$$u^4A' = A, \qquad u^6B' = B, \qquad u^{12}\Delta' = \Delta.$$

Indeed, we have that

$$\begin{aligned} y^2 &\mapsto u^6y^2; \\ x^3 &\mapsto u^6x^3; \\ Ax &\mapsto Au^2x \end{aligned}$$

hence the equation becomes

$$u^6y^2 = u^6x^3 + Au^2x + B$$

and multiplying it by u^{-6}, we obtain

$$y^2 = x^3 + u^{-4}Ax + u^{-6}B$$

hence

$$\begin{aligned} A' = u^{-4}A \quad &\iff \quad u^4A = A' \\ B' = u^{-6}B \quad &\iff \quad u^6B = B'. \end{aligned}$$

Then, we can also compute

$$\Delta' = -16(4(A')^3 + 27(B')^2) = -16(4u^{12}A^3 + 27u^{12}B^2) = u^{12}\Delta.$$

For a general Weierstrass equation, we can compute the values of each coefficient in the same way, but the computations are more tedious. The results for this are given in the Table 1 below.

(x, y)	$(u^2x + 3,\ u^3y + u^2sx + t)$
a_1	$ua_1' = a_1 + 2s$
a_2	$u^2a_2' = a_2 - sa_1 + 3r - s^2$
a_3	$u^3a_3' = a_3 + ra_1 + 2t$
a_4	$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
b_2	$u^2b_2' = b_2 + 12r$
b_4	$u^4b_4' = b_4 + rb_2 + 6r^2$
b_6	$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$
b_8	$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
c_4	$u^4c_4' = c_4$
c_6	$u^6c_6' = c_6$
Δ	$u^{12}\Delta' = \Delta$
j	$j' = j$
ω	$u^{-1}\omega' = \omega$

Table 1: Change of variables table for Weierstrass equations (adapted from [11, Table 3.1])

Proposition 4.8. *The following properties hold:*

(a) E is singular if and only if $\Delta = 0$, and

(i) it has a node if and only if $c_4 \neq 0$,

(ii) it has a cusp if and only if $c_4 = 0$;

(b) Two elliptic curves are isomorphic over $\bar{K}$ if and only if they both have the same j-invariant;

(c) For all $j_0 \in \bar{K}$ there exists an elliptic curve over $K(j_0)$ with its j-invariant j_0.

Proof. (a) Let E be a curve given by the Weierstrass equation

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

First, we show that the point at infinity $O = [0:1:0]$ is never singular. Therefore, we need to look at the curve on $\mathbb{P}^2(K)$ defined by the homogeneous equation

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

We have that

$$\frac{\partial F}{\partial Z}(X,Y,Z) = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2$$

hence

$$\frac{\partial F}{\partial Z}(O) = 1 \neq 0$$

so O is nonsingular.

Next, assume that E is singular at some $P_0 = (x_0, y_0)$. Now note that the substitution

$$x = x' + x_0, \qquad y = y' + y_0$$

leaves Δ and c_4 invariant hence we may assume, without loss of generality, that $P_0 = (0,0)$. Then, from $f(0,0) = 0$, we obtain $a_6 = 0$. Moreover, from

$$\frac{\partial f}{\partial x}(0,0) = \frac{\partial f}{\partial y}(0,0) = 0$$

and

$$\frac{\partial f}{\partial x}(x,y) = a_1y - 3x^2 - a_2x^2 - a_4,$$
$$\frac{\partial f}{\partial y}(x,y) = 2y + a_1x + a_3,$$

we obtain

$$a_4 = \frac{\partial f}{\partial x}(0,0) = 0,$$
$$a_3 = \frac{\partial f}{\partial y}(0,0) = 0.$$

Thus, E becomes

$$E : y^2 + a_1xy - a_2x^2 - x^3 = 0$$

for which we have

$$\begin{aligned} b_2 &= a_1^2 + 4a_4; \\ b_4 &= 0; \\ b_6 &= 0; \\ b_8 &= 0; \end{aligned}$$

hence $c_4 = (a_1^2 + 4a_4)^2$ and $\Delta = 0$.

Now, by Definition 4.4, E has a node at $P_0 = (0,0)$ if the quadratic form

$$y^2 + a_1 xy - a_2 x$$

has distinct factors, i.e., if the discriminant of the quadratic form is nonzero:

$$a_1^2 + 4a_4 \neq 0 \quad \Longleftrightarrow \quad c_4 \neq= 0.$$

On the other hand, the point $P_0 = (0,0)$ has a cusp if the quadratic form has equal factors, i.e if the discriminant of it is precisely 0. This shows that if $c_4 \neq 0$ and $\Delta = 0$, then we have a node, and if $c_4 = \Delta = 0$, a cusp.

To complete the rest of the proof, we will show that if E is nonsingular, then $\Delta \neq 0$. In order to avoid tedious computations, we shall assume that char $K \neq 2$, and thus, consider a Weierstrass equation for E of the form:

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6.$$

Then $P = (x_0, y_0)$ is singular if and only if

$$\begin{aligned} \frac{\partial}{\partial y} y^2 \mid_{(x_0,y_0)} = \frac{\partial}{\partial x}(4x^3 + b_2 x^2 + 2b_4 x + b_6) \mid_{(x_0,y_0)} &= 0 \\ 2y_0 = 12x_0^2 + 2b_2 x_0 + 2b_4 &= 0 \end{aligned}$$

hence the singular points are of the form $(x_0, 0)$ such that

$$4x_0^3 + b_2 x_0^2 + 2b_4 x_0 + b_6 = 0 \text{ and } 12x_0^2 + 2b_2 x_0 + 2b_4 = 0$$

hence x_0 is a double root of the cubic polynomial $4x_0^3 + b_2 x_0^2 + 2b_4 x_0 + b_6 = 0$. This polynomial has a double root if and only if its discriminant is equal to zero:

$$\begin{aligned} 0 &= 4b_2^2 b_4^2 - 4 \cdot 4 \cdot 8 \cdot b_4^3 - 4b_2^3 b_6 - 27 \cdot 16 \cdot b_6^2 + 18 \cdot 4 \cdot 2 \cdot b_2 \cdot b_4 \cdot b_6 \\ &= 4b_2^2(b_4^2 - b_2 b_6) - 16 \cdot 8 \cdot b_4^3 - 16 \cdot 27 \cdot b_6^2 + 16 \cdot 9 \cdot b_2 \cdot b_4 \cdot b_6 \\ &= 16(-b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6) \\ &= 16\Delta. \end{aligned}$$

This completes the proof.

(b) Assume that two elliptic curves E and E' with respective invariants j and j' are isomorphic. Then, there exists some change of variables as in (5) that maps all elements of E to E'. Then by Table 1, $j' = j$. Conversely, assume that E and E' have the same j-invariant. For simplicity, we assume that char $K \neq 2, 3$ so that we can write

$$\begin{aligned} E &: y^2 = x^3 + Ax + B \\ E' &: y^2 = x^3 + A'x + B' \end{aligned}$$

Then, by assumption

$$j = j' \iff \frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4(A')^3 + 27(B')^2} \iff 4A^3(A')^3 + 27A^3(B')^2 = 4A^3(A')^3 + 27(A')^3B^2$$

which gives

$$A^3(B')^2 = (A')^3B^2$$

Since we are in characteristic different than 2 or 3, we need to look for isomorphisms of the form

$$(x, y) \mapsto (u^2x, u^3y).$$

We distinguish between three cases:

I. $A = 0 \Rightarrow j = 0$
Since we cannot have $\Delta = 0$, it is necessary that $B \neq 0$. This in turn implies that $A' = 0$ since $(A')^3B^2 = 0$. Then for $u = (B/B')^{1/6}$, the equation for E becomes

$$\frac{B}{B'}y^2 = \frac{B}{B'}x^3 + A \cdot \left(\frac{B}{B'}\right)^{1/3} + B \iff y^2 = x^3 + A \cdot \left(\frac{B}{B'}\right)^{-2/3} + B'$$

and since

$$A^3(B')^2 = (A')^3B^2 \iff \frac{B^2}{B'^2} = \frac{A^3}{(A')^3} \iff \left(\frac{B}{B'}\right)^{-2/3} = \frac{A'}{A}$$

we obtain the equation for E'.

II. $B = 0 \Rightarrow j = 1728$
By the same argument as above, we obtain $A \neq 0$ and hence $B' = 0$. Thus if we take $u = (A/A')^{1/4}$, the equation for E becomes

$$\left(\frac{A}{A'}\right)^{3/2} y^2 = \left(\frac{A}{A'}\right)^{3/2} x^3 + A \cdot \left(\frac{A}{A'}\right)^{1/2} x + B \iff y^2 = x^3 + A \cdot \left(\frac{A}{A'}\right)^{-1} + B \cdot \left(\frac{A'}{A}\right)^{3/2}$$

From the first case it is easy to see that

$$B' = B \cdot \left(\frac{A'}{A}\right)^{3/2}$$

hence we have yet again obtained E'.

III. $AB \neq 0 \Rightarrow j \neq 0, 1728$
The above implies that $A'B' \neq 0$ must hold as well, since if one of them would be 0, then both A' and B' should be 0 from the equality $A^3(B')^2 = (A')^3B^2$. If both of them were 0, then $\Delta' = 0$ which is impossible. Thus, in this case we can take either of the values from the previous cases for u, hence E and E' are isomorphic and this concludes the proof.

(c) Similarly to the proof of (b), we consider three cases:

I. $j_0 \neq 1728, 0$
Consider the curve E given by the equation

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

We then compute

$$\begin{aligned}
b_2 &= 1^2 = 1 \\
b_4 &= 2 \cdot \frac{-36}{j_0 - 1728} = -\frac{72}{j_0 - 1728}; \\
b_6 &= -\frac{4}{j_0 - 1728}; \\
b_8 &= -1 \cdot \frac{1}{j_0 - 1728} - \frac{1296}{(j_0 - 1728)^2}; \\
c_4 &= 1 - 24 \cdot \frac{-72}{j_0 - 1728} = 1 + \frac{1728}{j_0 - 1728} = \frac{j_0}{j_0 - 1728};
\end{aligned}$$

which allows us to determine

$$\begin{aligned}
\Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \\
&= -\left(-\frac{1}{j_0 - 1728} - \frac{1296}{(j_0 - 1728)^2}\right) + 8 \cdot \frac{72^3}{(j_0 - 1728)^3} - 27 \cdot \frac{72^3}{(j_0 - 1728)^3} \\
&\quad - 27 \cdot \frac{16}{(j_0 - 1728)^3} + 9 \cdot \frac{4 \cdot 72}{(j_0 - 1728)^2} \\
&= \frac{(j_0 - 1728)^2 + 3456(j_0 - 1728) + 2985984}{(j_0 - 1728)^3} \\
&= \frac{j_0^2}{(j_0 - 1728)^3}
\end{aligned}$$

and hence,

$$j = \frac{c_4^3}{\Delta} = \frac{j_0^3}{(j_0 - 1728)^3} \cdot \frac{(j_0 - 1728)^3}{j_0^2} = j_0.$$

This yields an elliptic curve with j-invariant j_0 for all choices of j_0 subject to the condition that $j_0 \neq 0,\ 1728$.

II. $j_0 = 0$
Define

$$E : y^2 + y = x^3.$$

This curve has discriminant $\Delta = -27$ and $c_4 = 0$ thus, $j = 0$.

III. $j_0 = 1728$
Consider

$$E : y^2 = x^3 + x$$

with $\Delta = -64$ and $c_4 = -48$. Then

$$j = \frac{c_4^3}{\Delta} = \frac{-110592}{-64} = 1728.$$

We note that in the case we are in characteristic 2, case **II.** is singular, and if we are in characteristic 3, case **III.** is singular, but we need not worry as for both characteristics $0 = 1728$, and so, at least one of the two cases defines an elliptic curve.

□

4.1 Legendre form

Sometimes it is more convenient to write Weierstrass equations in a different form. In this section, we introduce the Legendre form,

Definition 4.9 (Legendre form)**.** *A Weierstrass equation is in Legendre form if it can be written as*

$$y^2 = x(x-1)(x-\lambda). \tag{6}$$

Proposition 4.10. *Assume that* $\mathrm{char}(K) \neq 2$*. Then*

(a) Every elliptic curve is isomorphic over $\bar{K}$ *to an elliptic curve in Legendre form*

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in \bar{K}$ *with* $\lambda \neq 0, 1$.

(b) The j-invariant of E_λ *is*

$$j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

Proof. (a) Note that $\mathrm{char}(K) \neq 2$, thus E has Weierstrass equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Consider

$$(x, y) \to (x, 2y)$$

which yields

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

hence we can factor the cubic on the right hand side and obtain an equation of the form

$$\begin{aligned} y^2 &= (x-e_1)(x-e_2)(x-e_3) \\ &= (x^2 - (e_1+e_2)x + e_1e_2)(x-e_3) \\ &= x^3 - (e_1+e_2+e_3)x^2 + (e_1e_2 + e_1e_3 + e_2e_3)x - e_1e_2e_3 \end{aligned}$$

for some $e_1, e_2, e_3 \in \bar{K}$. Moreover, one can easily compute

$$\Delta = 16(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2$$

and $\Delta \neq 0$, so it must be that e_1, e_2 and e_3 are pairwise distinct. Now, the coordinate change given by

$$x = (e_2-e_1)x' + e_1, \qquad y = (e_2-e_1)^{3/2}y'$$

gives

$$\begin{aligned} (e_2-e_1)^3(y')^2 &= ((e_2-e_1)x' + e_1 - e_1)((e_2-e_1)x' + e_1 - e_2)((e_2-e_1)x' + e_1 - e_3) \\ &= (e_2-e_1)^3 x'(x'-1)\left(x' - \frac{e_3-e_1}{e_2-e_1}\right) \end{aligned}$$

and dividing the above by $(e_2 - e_1)^3$ yields a new Weierstrass equation in Legendre form:

$$E : y^2 = x(x-1)(x-\lambda)$$

where $\lambda = \dfrac{e_3 - e_1}{e_2 - e_1} \in \bar{K}$, and $\lambda \neq 0, 1$ since $e_i \neq e_j$ for all $i \neq j$.

(b) Note that from (a), we have that

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

has discriminant

$$\Delta = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$$

and the change of variables with $u = (e_2 - e_3)^{\frac{1}{2}}$ gives us the Legendre form (6) with $\lambda = \dfrac{e_3 - e_1}{e_2 - e_1}$. Then, the discriminant Δ' of this form can be computed using Table 1:

$$\begin{aligned}
\Delta' &= (e_2 - e_1)^{-6}\Delta \\
&= \frac{16(e_2 - e_1)^2(e_1 - e_3)^2(e_2 - e_3)^2}{(e_2 - e_3)^6} \\
&= 16\lambda^2 \left(\frac{e_2 - e_1}{e_2 - e_1} - \frac{e_3 - e_1}{e_2 - e_1} \right)^2 \\
&= 16\lambda^2(1 - \lambda)^2
\end{aligned}$$

In order to determine the j-invariant, we need to also compute c_4. Expanding the Legendre form gives

$$E : y^2 = x^3 - (1 + \lambda)x^2 + \lambda x$$

hence, we have

$$\begin{aligned}
c_4 &= 4^2 \cdot (1 + \lambda)^2 - 24 \cdot 2\lambda \\
&= 16(1 + 2\lambda + \lambda^2 - 3\lambda) \\
&= 16(\lambda^2 - \lambda + 1).
\end{aligned}$$

Combining everything together then yields

$$j(E_\lambda) = \frac{c_4^3}{\Delta} = \frac{2^{12}(\lambda^2 - \lambda + 1)^3}{2^4\lambda^2(\lambda - 1)^2} = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

□

4.2 The Abelian Group of Elliptic Curves

The set of points satisfying the Weierstrass equation of an elliptic curve $E \subset \mathbb{P}^2$ forms an abelian group together with the point at infinity O serving as the identity element. This group structure arises from a geometric construction and can be expressed through explicit algebraic formulas.

Let E be an elliptic curve over a field K, given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with coefficients in K and point at infinity $O = [0, 1, 0]$.

Definition 4.11 (Group law on E)**.** *The composition law, here denoted by $+$, on E is defined as follows:*

- *Let P and Q be two points on E.*
- *Let L be the line through P and Q, or if $P = Q$,the tangent to E at P.*
- *Let R be the third point of intersection of L with E.*
- *Let L' be the line through R and O.*

Then $P + Q$ is defined as the third point of intersection of L' with E.

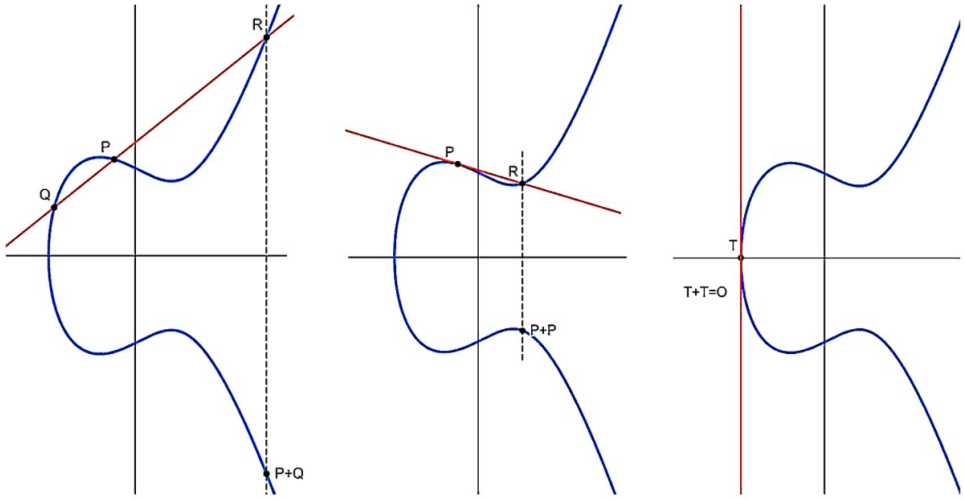

Figure 3: Group Law.

This composition law satisfies the axioms of an abelian group, with O as the identity element, and a unique inverse.

Proposition 4.12. *The triple $(E, +, O)$ forms an abelian group. That is,*

(a) $P + O = O + P = P$ *for all* $P \in E$*;*

(b) For all $P, Q, R \in E$

$$(P + Q) + R = P + (Q + R);$$

(c) For all $P \in E$*, there exists some point,* $Q := -P \in E$ *satisfying*

$$P + (-P) = O$$

(d) $P + Q = Q + P$ *for all* $P, Q \in E$*.*

Additionally, the composition law has the properties

(e) Let the line L intersect E at the points $P, Q, R \in E$. Then

$$(P + Q) + R = O$$

(f) If E is defined over K then $E(K)$ is a subgroup of $E(\bar{K})$ where

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

Proof. (a) This is quite clear by construction. In this case, if we take $Q = O$, the lines L and L' in Definition 4.11 coincide. The former intersect the elliptic curve at P, O, R, whereas the latter at R, O, $P + O$. Since a line can intersect the elliptic curve at no more than 3 points, this shows that $P + O = P$. To show that $O + P = P$, the reasoning is completely analogous.

(b) See Proposition 3.4.(e) in Chapter III from [11].

(c) Let the third point of intersection with E of the line through P and O be R. Using (e), we have

$$O = (P + O) + R = P + R.$$

(d) This follows immediately from the construction in Definition 4.11, which is symmetric in P and Q.

(e) This is easy to see from Definition 4.11. We have that $P + Q$ is given by the third point of intersection of the line through R and O and the elliptic curve. Thus, $P + Q$, R, O are collinear and since the tangent of E at O intersects E with multiplicity 3 at O, we obtain

$$(P + Q) + R = O.$$

(f) First, $E(K)$ is clearly a subset of $E(\bar{K})$. Next, we will check the subgroup axioms. The fact that $O \in E(K)$ is clear from the construction of $E(K)$. Now, let P, $Q \in E(K)$. Then, the equation of the line L through P and Q must have coefficients in K and thus the third point of intersection of L with the elliptic curve, which we denote by R, is also in $E(K)$. Denote the line through R and O by L'. Similarly as above, the third point of intersection of L' and E, i.e., $P + Q$ is in $E(K)$. Finally, note that we have $Q + R \in E(K)$, and so, $P + (Q + R) \in E(K)$. But by (b)

$$P + (Q + R) = (P + Q) + R$$

and since P, Q, $R \in E(K)$ are colinear, by (e) we obtain

$$(P + Q) + R = O$$

and hence, $O \in E(K)$.

□

Remark 4.13. *All properties except for (b) follow from the geometric construction, while (b) is more difficult to prove and is omitted here. A direct verification using explicit formulas is possible but lengthy; alternatively, one can use the Riemann–Roch Theorem (II.5.4 in [11]).*

We now derive explicit formulas for the group operations on E.

Proposition 4.14 (Inverse)**.** *Let $P = (x, y) \in E$. Then the inverse of P is given by*

$$-P = (x, -y - a_1x - a_3).$$

Proof. Consider some elliptic curve given by the implicit equation

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

and let $P = (x_0, y_0)$ and consider the line L through P and O and denote the third point of intersection with E by Q. Indeed,from the previous proposition we have

$$(P + O) + Q = O \qquad \Longleftrightarrow \qquad P + Q = O$$

hence $Q = -P$. Moreover, the line L is given by $x - x_0 = 0$. Substituting this into f yields $f(x_0, y) = 0$ where $f(x_0, y)$ is a quadratic polynomial in y with roots y_0 and y_0' and $-P = (x_0, y_0')$. Our goal is to compute y_0' in terms of x_0 and y_0. To this extent, notice that

$$f(x_0, y) = c(y - y_0)(y - y_0') = cy^2 - cyy_0' - cyy_0 + cy_0y_0'.$$

Now, by equating the coefficients of y^2 we obtain $c = 1$ and

$$-(y_0' + y_0)y = (a_1x_0 + a_3)y$$

hence $y_0' = -y_0 - a_1x_0 - a_3$. This finishes the proof. □

Proposition 4.15 (Addition)**.** *Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E.*

(a) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 + P_2 = O$.

(b) Otherwise, define the line through P_1 and P_2 (or the tangent if $P_1 = P_2$) by

$$L : y = \lambda x + \nu,$$

where:

$$\begin{cases} \text{If } x_1 \neq x_2, \text{ then } \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}, \nu = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}; \\ \\ \text{If } x_1 = x_2, \text{ then } \lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \nu = \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}. \end{cases}$$

Then the third point of intersection is $P_3 = (x_3, y_3')$, where:

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3' &= -(\lambda + a_1)x_3 - a_3 - \nu. \end{aligned}$$

Finally, $P_1 + P_2 = P_3$.

Proof. Note that (a) follows immediately from 4.14. It remains to show (b). Let L be the line through P_1 and P_2. Then L is of the form

$$L : y = \lambda x + \nu$$

and $f(x, \lambda x + \nu)$ has precisely three roots, x_1, x_2 and x_3, where we denote $-P_3 = (x_3, y_3)$. Since $-P_3$ is the additional point of intersection of L with E, from 4.12 we have

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

Then, as in the previous proof write

$$f(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$$

and by equating with the x^3 and x^2 terms yields

$$\begin{cases} cx^3 = -x^3 \\ cx^2(-x_3 - x_2 - x_1) = x^2(-a_2 + \lambda^2 + a_1\lambda) \end{cases} \iff \begin{cases} c = -1 \\ x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2 \end{cases}$$

Thence, we obtain $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_3 = \lambda x_3 + \nu$. Moreover, for $P_3 = (x_3, y_3')$, we have that $y_3' = -\lambda(x_3 + a_1)x_3 - a_3 - \nu$.
Now, assume that $x_1 \neq x_2$. Then, as $P_1, P_2 \in L$ we have

$$\begin{cases} y_1 = \lambda x_1 + \nu \\ y_2 = \lambda x_2 + \nu \end{cases}$$

from which we obtain

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{and} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

For $x_1 = x_2$, since we are in the case where $y_1 + y_2 + a_1 x_2 + a_3 \neq 0$, it must be that $P_1 = P_2$ and hence L is the tangent line to E at $P_1 = P_2$. After some straightforward computations we obtain

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \qquad \text{and} \qquad \nu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}.$$

□

4.3 Base change and twist

Let E/K be an elliptic curve defined over some field K, and L/K a finite extension of K. In this section, we explain the notions of base change and twist of an elliptic curve with respect to L. These concepts will prove to be extremely useful in the process of proving Theorem 5.3.

Recall that the Weierstrass equation of an elliptic curve E is unique up to the change of variables of the form

$$x = u^2 x' + r \qquad \text{and} \qquad y = u^3 y' + su^2 x' + t,$$

where $u, r, s, t \in \bar{K}$ with $u \neq 0$.

Definition 4.16 (Base change)**.** *Consider some elliptic curve E/K. The base change of E from K to L, denoted by E_L is defined to be an elliptic curve with coefficients in L such that E_L is isomorphic to E over the extension L, but not over K.*

Definition 4.17 (Twist)**.** *The twist E^L of an elliptic curve E/K is an elliptic curve with coefficients in K and isomorphic to E over L.*

Example 4.18 (Quadratic twist)**.** *Let E/K be some elliptic curve defined over K described by the Weierstrass equation:*

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Suppose that $L := K(\sqrt{d})$, with $\eta^2 = 1/d$ and $d \in K^\times$ square-free, is a quadratic extension of K. Then the quadratic twist of E by d is given by the coordinate change:

$$x = \eta^2 x \qquad \text{and} \qquad y = \eta^3 y' + \frac{a_1(\eta-1)}{2}\eta^2 x' + \frac{a_3(\eta^3-1)}{2}.$$

Denote the resulting curve by E' and a_i' for $i \in \{1,\dots,6\}$, its corresponding quantities. Note that $\sqrt{d} \in L$ and it is nonzero, hence, it is clear that $\eta = 1/\sqrt{d} \in L^\times$ since L is a field and d nonzero. Moreover, it also follows that $a_1(\eta-1)/2$, $a_3(\eta^3-1)/2 \in L$. This shows that E' is isomorphic to E over the extension L through the coordinate change (5).

Next, we compute each of the coefficients of E using the formulas in Table 1 and check that they are elements of K:

$$a_1' = \eta^{-1}(a_1 + a_1(\eta-1)) = a_1;$$

$$\begin{aligned} a_2' &= \eta^{-2}\left(a_2 - \frac{a_1^2(\eta-1)}{2} - \frac{a_1^2(\eta-1)^2}{4}\right) \\ &= d\left(a_2 - \frac{a_1^2(\eta-1)(2+\eta-1)}{4}\right) \\ &= d\left(a_2 - \frac{a_1^2(1/d-1)}{4}\right) \\ &= da_2 + \frac{a_1^2(d-1)}{4}; \end{aligned}$$

$$a_3' = \eta^{-3}(a_3 + a_3(\eta^3-1)) = a_3;$$

$$\begin{aligned} a_4' &= \eta^{-4}\left(a_4 - \frac{a_3a_1(\eta-1)}{2} - \frac{a_1a_3(\eta^3-1)}{2} - \frac{a_1a_3(\eta-1)(\eta^3-1)}{2}\right) \\ &= \frac{d^2}{2}(2a_4 - a_1a_3(\eta-1)(1 + (\eta^2+\eta+1) + (\eta^3-1)) \\ &= \frac{d^2}{2}(2a_4 - a_1a_3(\eta-1)(\eta^3+\eta^2+\eta+1) \\ &= \frac{d^2}{2}(2a_4 - a_1a_3(1/d^2-1)) \\ &= a_4d^2 + \frac{a_1a_3(d^2-1)}{2}; \end{aligned}$$

$$
\begin{aligned}
a_6' &= \eta^{-6}\left(a_6 - \frac{a_3^2(\eta^3-1)}{2} - \frac{a_3^2(\eta^3-1)^2}{4}\right) \\
&= d^3\left(a_6 - \frac{a_3^2(\eta^3-1)(2+\eta^3-1)}{4}\right) \\
&= a_6 d^3 + \frac{a_3^2(d^2-1)}{4}.
\end{aligned}
$$

From the above computations, we see that $a_i' \in K$, for all i. Thus, E' is the quadratic twist of E by d, and it is given by the equation:

$$
E' : y^2 + a_1xy + a_3y = x^3 + \left(a_2 d + \frac{a_1^2(d-1)}{4}\right)x^2 + \left(a_4 d^2 + \frac{a_1 a_3(d^2-1)}{2}\right)x + \left(a_6 d^3 + \frac{a_3^2(d^3-1)}{4}\right).
$$

4.4 Elliptic curves over local fields

Recall from Section 4, Proposition 4.8 that an elliptic curve is nonsingular if and only if its discriminant Δ is nonzero. That is, if $\Delta = 0$, the Weierstrass equation has a singular point.

Example 4.19. *Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation with coefficients in $\mathbb{Z}$. Since $\mathbb{Z}$ is a unique factorization domain we can write the discriminant as a unique product of prime factors, that is*

$$
\Delta = \prod_{i=1}^{n} p_i^{e_i}
$$

where $p_i \neq p_j$ for all $i \neq j$ and e_i is the multiplicity of the prime p_i in the factorization of Δ. A common technique is to reduce the coefficients of E modulo a prime p, thereby obtaining a curve defined over the finite field $\mathbb{F}_p$. For finitely many primes, in particular p_i for $i \in \{1, 2, \ldots, n\}$, one obtains $\Delta \equiv 0 \pmod{p}$ and thus, in $\mathbb{F}_{p_i}$, the reduced curve is no longer an elliptic curve. On the other hand, for a prime p such that $p \neq p_i$ for all i, the reduced curve is nonsingular, and thus an elliptic curve over $\mathbb{F}_p$.

This example illustrates the idea of reducing an elliptic curve modulo a prime to study its behavior over finite fields. To make this notion precise, we now introduce the general framework for studying elliptic curves over local fields, where the concept of reduction plays a central role in understanding the arithmetic of the curve at a given prime.

In this section, we consider K to be a local valued field with respect to v, a discrete valuation, O_K its ring of integers, $\mathfrak{m}$ the maximal ideal of O_K with uniformizer π, i.e., $\mathfrak{m} = (\pi)$, and $k = O_K/\mathfrak{m}$ the residue field of O_K. Moreover, we assume that v is normalized, that is, $v(\pi) = 1$.

4.4.1 The Minimal Weierstrass Equation

An elliptic curve E/K admits a Weierstrass equation of the form

$$
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{7}
$$

with $a_i \in K$. Let Δ denote its discriminant.

To study models over O_K, we consider coordinate changes of the form:

$$(x, y) \longmapsto (u^{-2}x, u^{-3}y).$$

This substitution yields

$$u^{-6}y^2 + u^{-5}a_1xy + u^{-3}a_3y = u^{-6}x^3 + u^{-4}a_2x^2 + u^{-2}a_4x + a_6,$$

and multiplying both sides by u^6 gives the new equation:

$$y^2 + ua_1xy + u^3a_3y = x^3 + u^2a_2x^2 + u^4a_4x + u^6a_6 \tag{8}$$

Thus, each coefficient a_i is replaced by u^ia_i, and if we choose u such that it is divisible by a sufficiently large power of π, we obtain a Weierstrass equation with all its coefficients in O_K. Indeed, assume that $a_i = \dfrac{c}{\pi^m}$ with $\pi \nmid c$, and let u be divisible by π^n where $n \geqslant m$. Then,

$$v(u^ia_i) = in - m \geqslant 0, \qquad \forall i$$

hence $u^ia_i \in O_K$. In this case, the discriminant of (8) is given by

$$\begin{aligned}\Delta' &= (u^2a_1^2 + 4u^2a_2)^2(u^8a_1a_6 + 4u^8a_2a_6 - u^8a_1a_3a_4 + u^8a_2a_3^2 - u^8a_4^2) - 8(2u^4a_4 + u^4a_1a_3)^3 - \\ &\quad - 27(u^6a_3^2 + 4u^6a_6)^2 + 9(u^2a_1^2 + 4u^2a_2)(2u^4a_4 + u^4a_1a_3)(u^6a_3^2 + 4u^6a_6)\\ \\ &= u^{12}[-(a_1^2 + 4a_2)^2(a_1a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2) - 8(2a_4 + a_1a_3)^3 - \\ &\quad - 27(a_3^2 + 4a_6)^2 + 9(a_1^2 + ua_2)(2a_4 + a_1a_3)(a_3^2 + 4a_6)] = u^{12}\Delta\end{aligned}$$

Therefore, by choosing u with suitable valuation, one can minimize $v(\Delta)$.

Definition 4.20 (Minimal Weierstrass equation)**.** *A Weierstrass equation for E/K is said to be* minimal at v *if $v(\Delta)$ is minimized subject to the condition that $a_i \in O_K$. The minimal value of $v(\Delta)$ is said to be the* valuation of the minimal discriminant of E *at v.*

Now, in order to find a minimal equation we must have $a_i \in O_K$ for all i by definition. Suppose that E/K is such that this holds, but not minimal. In section 4 we saw that a Weierstrass equation is unique up to the coordinate change

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + su^2x' + t, \qquad\qquad r, s, t \in \bar{K}, u \neq 0.$$

Proposition 4.21. *Let E/K be an elliptic curve.*

(i) If $a_i \in O_K$ and $v(\Delta) < 12$, the Weierstrass equation for E is minimal.

(ii) If $a_i \in O_K$ and $v(c_4) < 4$, the Weierstrass equation for E is minimal.

(iii) If $a_i \in O_K$ and $v(c_6) < 6$, the Weierstrass equation for E is minimal.

Proof. From Table 1 we know that with the substitution above yields a new discriminant $\Delta' = u^{-12}\Delta$. Hence, $v(\Delta)$ can only be changed by multiples of 12. Similarly, since $c_4' = u^{-4}c_4$ and $c_6' = u^{-4}c_6$, then $v(c_4)$ and $v(c_6)$ can only be changed by multiples of 4 and 6 respectively. □

Example 4.22. *Let E be an elliptic curve, with Weierstrass equation*

$$E : y^2 = x^3 - 412x - 3316.$$

with discriminant $\Delta = -1 \cdot 2^8 \cdot 5^5 \cdot 7^3$. The Weierstrass equation is minimal over $\mathbb{Q}_p$ for all primes. Indeed, all coefficients of the equation are elements of $\mathbb{Z}_p$, and moreover, for $p \neq 2, 5, 7$ we have:

$$v_p(\Delta) = 0 < 12,$$

for $p = 2$:

$$v_2(\Delta) = 8 < 12,$$

for $p = 5$:

$$v_5(\Delta) = 5 < 12$$

and for $p = 7$:

$$v_7(\Delta) = 3 < 12.$$

Determining whether a given Weierstrass equation is minimal can be subtle. A systematic procedure to compute minimal models is provided by *Tate's algorithm*, which is discussed in [12, p. IV.9.4]. The following proposition ensures us of the existence of a minimal Weierstrass equation for any elliptic curve defined over some local field, and moreover, it provides us with some useful properties.

Proposition 4.23. *Let E/K be an elliptic curve over a local field.*

(a) E admits a minimal Weierstrass equation;

(b) Any two minimal Weierstrass equations are related by a change of variables

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + su^2x' + t$$

with $u \in O_K^\times$ and $r, s, t \in O_K$;

(c) The invariant differential $\omega = \dfrac{dx}{2y + a_1x + a_3}$ is unique up to multiplication by an element of $O_K^\times$;

(d) Conversely, any change of variables

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + su^2x' + t$$

producing another minimal equation satisfies $u, r, s, t \in O_K$.

Proof. (a) We have seen in the beginning of the section that it is possible to obtain a Weierstrass equation with all coefficients in O_K after some change of variable Moreover, since any change of coordinate yields

$$v(\Delta') = v(u^{12}\Delta) = v(\Delta) + 12v(u),$$

where Δ' is the newly obtained discriminant, we can vary the power of π in u to ensure that the coefficients lie in O_K. Among all such equations, the valuation $v(\Delta')$ is minimized for some choice since v is discrete, yielding a minimal Weierstrass equation.

(b) Let E/K and E'/K be isomorphic. Then, there exists a change of variables of the form (5), with u, r, s, $t \in K$ and $u \neq 0$ between the two. Minimality of both equations implies $v(\Delta) = v(\Delta')$. Now, from Table 1, we have

$$u^{12}\Delta' = \Delta$$

hence

$$v(\Delta') = v(\Delta) = 12v(u) + v(\Delta') \quad \Rightarrow \quad v(u) = 0$$

giving that $u \in O_K^\times$. Next, again from Table 1

$$u^6 b_6' = b_6 + 2rb_4 + r^2 b_2 + 4r^3$$

and so we need

$$v(b_6 + 2rb_4 + r^2 b_2 + 4r^3) \geqslant 0.$$

Note that

$$v(b_6 + 2rb_4 + r^2 b_2 + 4r^3) \geqslant \min\{v(b_6),\, v(2r) + v(b_4),\, 2v(r) + v(b_2),\, v(4r^3)\}$$

by applying the second property of valuations four times. Assume that $v(r) < 0$. Then, since $v(b_i) \geqslant 0$ for all i,

$$\min\{v(b_6),\, v(2r) + v(b_4),\, 2v(r) + v(b_2),\, v(4r^3)\} = v(4r^3) < 0$$

which is a contradiction as we need $b_6' \in O_K$. Thus, we need $v(r) \geqslant 0$, and hence $r \in O_K$. From $a_2' \in O_K$ and

$$u^2 a_2' = a_2 - sa_1 + 3r - s^2$$

we get $s \in O_K$, and from $a_6 \in O_K$ and

$$u^6 a_6 = a_6 + ra_4 + r^3 a_2 + r^3 - ta_3 - t^2 - rta_1$$

that $t \in O_K$, hence we are done.

(c) This follows from the fact that $u \in O_K^\times$ and Table 1, since $\omega' = u\omega$.

(d) We have $u^{12}\Delta' = \Delta$ and since we also have obtained a minimal equation, $v(\Delta') \leqslant v(\Delta)$ so

$$12v(u) + v(\Delta') = v(\Delta) \geqslant v(\Delta') \quad \Rightarrow \quad v(u) \geqslant 0$$

hence $u \in O_K$. In order to show that r, s, $t \in O_K$, the proof is analogous to (b).

□

4.4.2 Reduction

In this section, we study how elliptic curves behave under reduction modulo the maximal ideal of a local field. This concept is central to understanding the arithmetic of elliptic curves at primes of bad reduction.

Let E/K be an elliptic curve defined over a local field K equipped with a discrete valuation v. Consider the minimal Weierstrass equation for E/K. Since the coefficients a_i lie in O_K, we may reduce them modulo the maximal ideal $\mathfrak{m} = (\pi)$ to obtain an equation over the residue field $k = O_K/\mathfrak{m}$. Let $\bar{a}_i$ denote the image of a_i in k, and define the *reduced curve* $\tilde{E}/k$ by:

$$\tilde{E} : y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6. \tag{9}$$

Definition 4.24 (Reduction modulo π)**.** *The curve $\tilde{E}/k$ defined by* (9) *is called the* reduction of E modulo π.

Similarly, for $P \in E(K)$ with homogeneous coordinates $P = [x_0, y_0, z_0]$ with $x_0, y_0, z_0 \in O_K$ and at least one $x_0, y_0, z_0 \in O_K^\times$, the reduced point $\tilde{P} = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}]$ is in $\tilde{E}(k)$. This defines a *reduction map*

$$E(K) \longrightarrow \tilde{E}(k), \qquad P \longmapsto \tilde{P}.$$

Definition 4.25 (Good Reduction)**.** *The elliptic curve E/K has* good reduction *at v if $\tilde{E}/k$ is a nonsingular curve.*

Remark 4.26. *Good reduction occurs if the reduction of the discriminant Δ satisfies $\tilde{\Delta} \neq 0$, or if $v(\Delta) = 0$ for a minimal Weierstrass equation.*

Example 4.27. *Let E be an elliptic curve with minimal Weierstrass equation*

$$E : y^2 = x^3 - 412x - 3316.$$

The discriminant of E is given by $\Delta = -1 \cdot 2^8 \cdot 5^5 \cdot 7^3$. Now, consider E over $\mathbb{Q}_{11}$. Then $\tilde{E}/k$ is given by

$$\tilde{E} : y^2 = x^3 - 5x - 5$$

so,

$$\tilde{\Delta} = -1 \cdot 2 \cdot 3$$

hence, $v(\Delta) = 0$, implying that $\tilde{E}/k$ is nonsingular. Therefore, the curve E has good reduction over $\mathbb{Q}_{11}$. In fact, E has good reduction over all $p \neq 2, 5, 7$ since

$$v_p(\Delta) = v_p(-1 \cdot 2^8 \cdot 5^5 \cdot 7^3) = 0, \qquad \forall p \neq 2, 5, 7.$$

Definition 4.28 (Bad Reduction)**.** *If $\tilde{E}/k$ is singular, we say that E/K has* bad reduction *at v.*

Bad reduction falls into two distinct types, depending on the nature of the singularity of the reduced curve $\tilde{E}$:

(i) **Multiplicative reduction:** If $\tilde{E}/k$ has a node, then E has *multiplicative reduction*. In this case, the reduced curve is a singular curve with a node.

(ii) **Additive reduction:** If $\tilde{E}/k$ has a cusp, then E has *additive reduction*. In this case, the reduced curve is a singular curve with a cusp.

Remark 4.29. *Bad reduction occurs when $v(\Delta) > 0$ (i.e., $\Delta \in \mathfrak{m}$), and the nature of the singularity can be detected by the value of c_4 modulo π:*

(a) If $v(c_4) = 0$, i.e., $c_4 \in O_K$, then $\tilde{E}$ has a node $\Rightarrow$ multiplicative reduction;

(b) If $v(c_4) > 0$, i.e., $c_v \in \mathfrak{m}$, then $\tilde{E}$ has a cusp $\Rightarrow$ additive reduction.

Example 4.30. *Consider the elliptic curve from 4.4.2 with minimal Weierstrass equation*

$$E : y^2 = x^3 - 412x - 3316$$

and discriminant $\Delta = -1 \cdot 2^8 \cdot 5^5 \cdot 7^3$.

Over $\mathbb{Q}_5$ and $\mathbb{Q}_7$ the curve has multiplicative reduction. Indeed,

$$v_5(\Delta) = 5 > 0 \qquad \textit{and} \qquad v_5(c_4) = v_5(2^2 \cdot 103 \cdot 3^{-3}) = 0$$

and

$$v_7(\Delta) = 3 > 0 \qquad \textit{and} \qquad v_7(c_4) = v_7(2^2 \cdot 103 \cdot 3^{-3}) = 0.$$

Over $\mathbb{Q}_2$ we have

$$v_2(\Delta) = 8 > 0 \qquad \textit{and} \qquad v_2(c_4) = v_2(2^2 \cdot 103 \cdot 3^{-3}) = 2 > 0$$

hence the reduction is additive.

Suppose that E/K is an elliptic curve having bad reduction. It is often useful to know whether it may attain good reduction over some extension of K. To this extent, we introduce the concept of *potential good reduction*.

Definition 4.31. *Let E/K be an elliptic curve. We say that E/K has* potential good reduction *if there exists a finite extension K'/K such that E has good reduction over K'.*

One natural question is whether bad reduction persists under field extensions. The following result, known as the *Semistable reduction theorem*, gives a partial answer.

Proposition 4.32 (Semistable reduction theorem)**.** *Let E/K be an elliptic curve.*

(a) Let K'/K be an unramified extension. Then the reduction type of E over K is the same as the reduction type of E over K'.

(b) Let K/K' be a finite extension. If E has either good or multiplicative reduction over K, then it has the same reduction type over K'.

(c) There exists a finite extension K'/K such that E has either good or multiplicative reduction over K'.

Proof. (a) We only prove this for $\mathrm{char}(k) \geqslant 5$. Note that the proof for arbitrary characteristic follows from Tate's algorithm (see IV.9 in [12]). Since $\mathrm{char}(k) \neq 2, 3$, we have that E/K has minimal Weierstrass equation of the form

$$E : y^2 = x^3 + Ax + B.$$

Consider $\mathcal{O}_{K'}$ and denote by v' the valuation on K' extending v on K. Now, let

$$x = (u')^2 x', \qquad y = (u')^3 y',$$

be some change of variables producing a minimal equation for E over K'. Since K/K' is unramified, the valuation v' on K' is an extension of v on K with

$$v(\pi) = v'(\pi) = 1$$

so there exists some $u \in K$ such that $v\left(\dfrac{u}{u'}\right) = 0$ and hence $\dfrac{u}{u'} \in \mathcal{O}_{K'}^{\times}$. Thus, as

$$v'(u) = v'(u') \qquad \Longleftrightarrow \qquad v(u^{-12}\Delta) = v((u')^{-12}\Delta),$$

the coordinate change

$$x - u^2x', \qquad y = u^3y'$$

also produces a minimal equation for E over K'. But then, this new equation has all of its coefficients in O_K and since the original equation is minimal over K, it must be that $v(u) = 0$. This shows that the original equation is also minimal over K'. Moreover, we have obtained that $v(\Delta) = v'(\Delta)$ and that $v(c_4) = v'(c_4)$, thus from Remark 4.29 we see that E has indeed the same reduction type over K' as it has over K. This shows (a).

(b) Now, take some minimal Weierstrass equation for E over K with Δ and c_4 its corresponding quantities. Existence of such a minimal equation is insured by Proposition 4.23.
Consider $O_{K'}$ and v', and let

$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t$$

be a substitution giving a minimal Weierstrass equation for E over K', with Δ' and c_4' the associated quantities to this new equation. Then we have

$$0 \leqslant v'(\Delta') = v'(u^{-12}\Delta)$$

and

$$0 \leqslant v'(c_4') = v'(u^{-4}c_4)$$

and from Proposition 4.23 (d), $u \in O_{K'}$ hence

$$0 \leqslant v'(u) \leqslant \min\left\{\frac{1}{12}v'(\Delta), \frac{1}{4}v'(c_4)\right\}.$$

Suppose first that E has good reduction over K. Then, $v(\Delta) = 0$ which implies that $v'(u) = 0$. Similarly, if E has multiplicative reduction, $v'(u) = 0$ since $v(c_4) = 0$. Then, it must be that

$$v'(\Delta') = v'(\Delta)$$

and

$$v'(c_4') = v'(c_4).$$

Then, if E/K has good reduction, $0 = v'(\Delta) = v'(\Delta')$ so E/K' has good reduction as well. Analogously, if E/K has multiplicative reduction, $v'(\Delta') = v'(\Delta) > 0$ and $v'(c_4') = v'(c_4) = 0$, so E/K' has multiplicative reduction. This finalizes the proof for (b).

(c) Assume that $\mathrm{Char}(k) \neq 2$, for the proof in $\mathrm{char}(k) - 2$ see Corollary 1.4. (a) in Appendix A of [11]. Let K'/K be a finite extension such that E/K' is defined by a Weierstrass equation in Legendre form:

$$E : y^2 = x(x-1)(x-\lambda),$$

where $\lambda \neq 0, 1$. The associated invariants of this model are:

$$c_4 = 16(\lambda^2 - \lambda + 1) \qquad \text{and} \qquad \Delta = 16\lambda^2(\lambda - 1).$$

We distinguish in between three cases.

(i) Suppose that $\lambda \in O_K$ and $\lambda \not\equiv 0, 1 \pmod{\mathfrak{m}}$. This means that $\Delta \not\equiv 0 \pmod{\mathfrak{m}}$ and hence, the equation has good reduction.

(ii) Assume now that $\lambda \in \mathcal{O}_K$
and $\lambda \equiv 0, 1 \pmod{\mathfrak{m}}$. Then, $\Delta \equiv 0 \pmod{\mathfrak{m}}$ and $c_4 \not\equiv 0 \pmod{\mathfrak{m}}$, hence $\Delta \in \mathfrak{m}$ and $c_4 \in \mathcal{O}_K^\times$, showing that E has multiplicative reduction.

(iii) Consider $\lambda \notin \mathcal{O}_K$ and let $r \geqslant 1$ such that $\pi^r \lambda \in \mathcal{O}_K^\times$. Then, consider the substitutions

$$x = \pi^{-r} x', \qquad y = \pi^{-3r/2} y'$$

where we can replace K by $K(\sqrt{\pi})$ in the case that r is an odd integer. This substitution yields the Weierstrass equation

$$\pi^{-3r}(y')^2 = \pi^{-r}x'(\pi^{-r}x' - 1)(\pi^{-r}x' - \lambda) \iff (y')^2 = x'(x' - \pi^r)(x' - \pi^r\lambda).$$

The equation above clearly has coefficients in $\mathcal{O}_K$ and moreover,

$$\Delta' = 16 \cdot \pi^{2r} \cdot \pi^{2r}\lambda^2(\pi^r - \pi^r\lambda)^2 = 16\pi^{6r}\lambda^2(1-\lambda)^2 \in \mathfrak{m},$$

and

$$c_4' = 16\pi^{6r}(\lambda^2 - \lambda + 1)^2 \Rightarrow c_4 \in \mathcal{O}_K^\times$$

hence E has multiplicative reduction and we are done.

□

The proposition below characterizes when an elliptic curve attains good reduction after a finite extension.

Proposition 4.33. *Let E/K be an elliptic curve. Then E has potential good reduction if and only if its j-invariant is integral; that is, $j(E) \in \mathcal{O}_K$.*

Proof. Yet again, we assume that $\mathrm{char}(k) \neq 2$. For the proof of $\mathrm{char}(k) = 2$ see Corollary 1.4. (b) in Appendix A of [11]. Let K' be a finite extension of K such that E has a Weierstrass equation in Legendre form

$$E : y^2 = x(x-1)(x-\lambda), \qquad \lambda \neq 0, 1.$$

and assume that $j(E) \in \mathcal{O}_K$. Then, from Proposition 4.10 (b) we know

$$j = 256\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2} \iff 256(1 - \lambda(1-\lambda))^3 - j\lambda^2(1-\lambda)^2 = 0$$

Using the fact that $j \in \mathcal{O}_K$ and the equality above, it must be that $\lambda \in \mathcal{O}_K$ since it is the root of a monic polynomial with integral coefficients, and $\lambda \neq 0, 1 \pmod{\mathfrak{m}}$. Hence, the Legendre equation over K' has good reduction.

Now, assume that E has potential good reduction over some field K'/K. Consider $\mathcal{O}_{K'}$ its ring of integers and Δ' and c_4' to some minimal Weierstrass equation for E over K'. Now, we have that $\Delta' \in \mathcal{O}_{K'}^\times$ since E/K' has good reduction, and thus

$$j(E) = \frac{(c_4')^3}{\Delta'} \in \mathcal{O}_{K'}$$

since $c_4 \in \mathcal{O}_K \subset \mathcal{O}_{K'}$, but E is defined over K so $j(E) \in K$, implying that $j(E) \in \mathcal{O}_K$. □

5 Acquiring good reduction

In this section, we explore how elliptic curves acquire good reduction through extensions of both local and number fields. We begin with an elliptic curve $E/\mathbb{Q}$ such that it has potentially good reduction at p, and study the minimal degree of a local extension $K/\mathbb{Q}_p$ over which E attains good reduction.

After analyzing the local setting, we turn our attention to the global question: Can an elliptic curve over $\mathbb{Q}$ acquire good reduction at *all* primes after a base change to a quadratic field? We will show that the answer is negative, that is, no such base change exists for any elliptic curve defined over $\mathbb{Q}$.

Finally, we present some examples of elliptic curves over $\mathbb{Q}$ that do acquire good reduction everywhere after a base change to cubic, quartic and sextic fields respectively, showing how such extensions can exist in higher degrees.

To set the stage, we begin by introducing the notion of the conductor of an elliptic curve and reviewing the classification of reduction types (Kodaira types), along with their relation to the conductor and other invariants of the curve.

Let $E/\mathbb{Q}$ be an elliptic curve. The conductor of $E/\mathbb{Q}$, denoted by $\mathrm{Cond}(E)$ is an integral ideal of K that encodes the primes of bad reduction. The following definition for $\mathrm{Cond}(E)$ is rather incomplete but suffices for our purposes. Write

$$\mathrm{Cond}(E) = \prod_{p \text{ prime}} p^{f_p(E)},$$

where, for $p \geqslant 5$,

$$f_p(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

In the case that $p = 2$ or 3, if E has additive reduction, then $f_p(E)$ can be greater than 2, but it is always the case that $f_3(E) \leqslant 3$ and $f_2(E) \leqslant 5$. For a complete definition of the conductor we refer to Chapter IV, Section 10 of [12].

Kodaira symbols classify the type of reduction an elliptic curve has at a prime where it does not have good reduction. We denote the type of reduction at some prime $\mathfrak{p}$ by $\mathrm{Type}(E, \mathfrak{p})$. Each symbol encodes both the structure of the singularities and the complexity of the bad reduction. This classification reflects how the curve degenerates at that prime, and it determines the local contribution to the conductor.

Below, we present part of the reduction type table (Table 15.1 in [11]). The values of $v(c_4)$ and $v(c_6)$ are taken from Table I in [8].

Kodaira symbol	I_0	I_n	II	III	IV	I_0^*	I_n^*	IV^*	III^*	II^*
$\mathrm{char}(k) = p$			$p \neq 2, 3$	$p \neq 2$	$p \neq 3$	$p \neq 2$	$p \neq 2$	$p \neq 3$	$p \neq 2$	$p \neq 2, 3$
$v(c_4)$	0 or $\geqslant 0$	0	$\geqslant 1$	1	$\geqslant 2$	2 or $\geqslant 2$	2	$\geqslant 3$	3	$\geqslant 4$
$v(c_6)$	$\geqslant 0$ or 0	0	1	$\geqslant 2$	2	$\geqslant 3$ or 3	3	4	$\geqslant 5$	5
$v_p(\Delta)$	0	n	2	3	4	6	$6+n$	8	9	10
$v_p(\mathrm{Cond}(E))$	0	1	2	2	2	2	2	2	2	2
behaviour of j	$v(j) \geqslant 0$	$\mathrm{ord}_v(j) = -n$	$\tilde{j} = 0$	$\tilde{j} = 1728$	$\tilde{j} = 0$	$v(j) \geqslant 0$	$\mathrm{ord}_v(j) = -n$	$\tilde{j} = 0$	$\tilde{j} = 1728$	$\tilde{j} = 0$

Table 2: Reduction types

5.1 Minimal degree of local extension for potential good reduction

Let E be an elliptic curve over $\mathbb{Q}_p$. Assume that E has potential good reduction at the prime p and K is the smallest degree field extension of $\mathbb{Q}_p$ where E/K has good reduction. What is the minimal degree $[K : \mathbb{Q}_p]$? To answer this question, we introduce the following result:

Theorem 5.1. *Let $E/\mathbb{Q}_p$ be an elliptic curve with potential good reduction, and assume $p > 3$. Consider a minimal Weierstrass equation for $E/\mathbb{Q}_p$ of the form,*

$$E : y^2 = x^3 + Ax + B, \qquad A,\, B \in \mathbb{Z}_p.$$

Then, the change of variables that yields good reduction is of the form:

$$(x,\, y) \mapsto (u^{-2}x, u^{-3}y)$$

with $u = \pi^r \in \mathcal{O}_K$ for some finite extension $K/\mathbb{Q}_p$, and

$$r = \min\left\{\frac{1}{4}v_p(A),\, \frac{1}{6}v_p(B)\right\}.$$

Remark 5.2. *Before proving the theorem, we note that Proposition 4.23 guarantees the existence of a minimal equation of $E/\mathbb{Q}_p$. Thus, we may assume that such an equation is always available.*

Proof. Denote the discriminant of $E/\mathbb{Q}_p$ by Δ and choose p as a uniformizer. Let $(x,\, y) \mapsto (u^2x, u^3y)$ be the change of variables such that E acquires good reduction at p over some finite extension $K/\mathbb{Q}_p$. Since E has bad reduction at p we have that $v_p(\Delta) > 0$. For good reduction we need the discriminant of the base change curve to have valuation identically zero thus, it is enough to modify Δ by factors of p, i.e, to take $u = p^r$ for some r such that $p^r \in K$. Moreover, since we need this new equation to be minimal as well, we have to take $u = p^r \in \mathcal{O}_K$ by Proposition 4.23 (b). Then the equation becomes

$$E' : y^2 = x^3 + u^{-2}Ax + u^{-6}B, \qquad u = p^r \in \mathcal{O}_K$$

where we denote its discriminant by Δ'. We shall prove that this coordinate change is as above constructively, depending on the type of reduction of E at p. First, we note that by Proposition 4.32, if E has potential good reduction at p, then it must be that E has additive reduction at p. Thus, using Table 2, we look at $\text{Type}(E,\, p) := \text{Type}(E)$ case by case and exclude the cases where $\text{Type}(E) = I_n$, with $n > 0$ since in this case we have multiplicative reduction, and $\text{Type}(E) = I_n^*$ where $n > 0$ as in this case the curve does not have potential good reduction by Proposition 4.33. First, note that in each of the cases, any change of variables needs to yield $v_p(\Delta') = 0$, thus we have

$$0 = v_p(\Delta') = v_p(u^{-12}) + v_p(\Delta) \iff v_p(u^{12}) = v_p(\Delta)$$

and substituting $u = p^r$ gives

$$v_p(p^{12r}) = v_p(\Delta) \iff 12r = v_p(\Delta) \iff r = \frac{v_p(\Delta)}{12.}$$

I. $\text{Type}(E) = II$.
From Table 2, we have $v(A) \geqslant 1$, $v(B) = 1$ and $v(\Delta) = 2$. Moreover, it is rather easy to see that

$$\min\left\{\frac{1}{4}v_p(A),\, \frac{1}{6}v_p(B)\right\} = \frac{1}{6}$$

and

$$r = \frac{v_p(\Delta)}{12} = \frac{1}{6}.$$

Therefore, $K = \mathbb{Q}_p(p^{1/6})$

II. Type$(E) = III$.
From Table 2, $v_p(A) = 1$, $v_p(B) = 2$ and $v_p(\Delta) = 3$. Compute

$$\min\left\{\frac{1}{4}v_p(A),\ \frac{1}{6}v_p(B)\right\} = \frac{1}{4}.$$

Then we have

$$r = \frac{v_p(\Delta)}{12} = \frac{1}{4}$$

hence $K = \mathbb{Q}_p(p^{1/4})$.

III. Type$(E) = IV$.
Table 2 gives us $v_p(A) \geqslant 2$, $v_p(B) = 2$ and $v_p(\Delta) = 4$. Then

$$\frac{1}{4} \geqslant \frac{1}{6} \quad \Rightarrow \quad \min\left\{\frac{1}{4}v_p(A),\ \frac{1}{6}v_p(B)\right\} = \frac{1}{3}.$$

From $v(\Delta') = 0$, we have

$$r = \frac{v_p(\Delta)}{12} = \frac{1}{3}$$

Then, $K = \mathbb{Q}_p(p^{1/3})$.

IV. Type$(E) = I_0^*$.
We have that $v_p(A) = 2$ or $\geqslant 2$, $v_p(B) \geqslant 3$ or $= 3$ and $v_p(\Delta) = 6$, and hence, we find

$$r = \frac{v_p(\Delta)}{12} = \frac{1}{2}.$$

First, we consider $v_p(A) = 2$ and $v_p(B) \geqslant 3$. Then we have

$$\min\left\{\frac{1}{4}v_p(A),\ \frac{1}{6}v_p(B)\right\} = \frac{1}{2}$$

If $v_p(A) \geqslant 2$ and $v_p(B) = 3$, we note that

$$\min\left\{\frac{1}{4}v_p(A),\ \frac{1}{6}v_p(B)\right\} = \frac{1}{2}$$

as well which yields that E acquires good reduction over $K = \mathbb{Q}_p(p^{3/6})$.

V. Type$(E) = IV^*$.
Table 2 gives $v_p(A) \geqslant 3$, $v_p(B) = 4$ and $v_p(\Delta) = 8$. As in the other cases, compute

$$\min\left\{\frac{1}{4}v_p(A),\ \frac{1}{6}v_p(B)\right\} = \frac{2}{3}$$

since $\frac{1}{4}v_p(A) \geqslant \frac{3}{4} \geqslant \frac{2}{3}$. From $v_p(\Delta') = 0$:

$$r = \frac{v_p(\Delta)}{12} = \frac{2}{3}$$

Hence, $K = \mathbb{Q}_p(p^{2/3})$.

VI. Type$(E) = III^*$.
In this case, $v_p(A) = 3$, $v_p(B) \geqslant 5$ and $v_p(\Delta) = 9$ and we note that

$$\min\left\{\frac{1}{4}v_p(A),\ \frac{1}{6}v_p(B)\right\} = \frac{3}{4}$$

since $\frac{1}{6}v_p(B) \geqslant \frac{5}{6} \geqslant \frac{3}{4}$. The fact that $v_p(\Delta') = 0$ gives

$$r = \frac{v_p(\Delta)}{12} = \frac{3}{4}$$

which yields that $K = \mathbb{Q}_p(p^{3/4})$.

VII. Type$(E) = II^*$.
Here, $v_p(A) \geqslant 4$, $v_p(B) = 5$ and $v_p(\Delta) = 10$. Now,

$$\min\left\{\frac{1}{4}v_p(A),\ \frac{1}{6}v_p(B)\right\} = \frac{5}{6}$$

as $\frac{1}{4}v_p(A) \geqslant \frac{4}{4} = 1 \geqslant \frac{5}{6}$. Since $v_p(\Delta') = 0$,

$$r = \frac{v_p(\Delta)}{12} = \frac{5}{6}$$

Thus, $K = \mathbb{Q}_p(p^{5/6})$.

This case-by-case analysis completes the proof □

Therefore, we found a transformation such that E acquires good reduction at p over a finite extension $K/\mathbb{Q}_p$, with $p > 3$. Summarizing the results that we found in the proof above for each reduction type yields:

Type	II	III	IV	I_0^*	IV^*	III^*	II^*
K	$\mathbb{Q}_p(p^{1/6})$	$\mathbb{Q}_p(p^{1/4})$	$\mathbb{Q}_p(p^{2/6})$	$\mathbb{Q}_p(p^{2/6}) = \mathbb{Q}_p(p^{3/6})$	$\mathbb{Q}_p(p^{4/6})$	$\mathbb{Q}_p(p^{3/4})$	$\mathbb{Q}_p(p^{5/6})$
$[K:\mathbb{Q}_p]$	6	4	3	2	3	4	6

Therefore, if $E/\mathbb{Q}$ has potentially good reduction at $p > 3$ then depending on the reduction type of E at p, the minimal degree of a local extension $K/\mathbb{Q}_p$ such that E/K has good reduction at p, can be found in the table above. For $p = 2, 3$, we refer the reader to the discussion in Section 2 of [5].

As discussed in this section, it is possible to construct elliptic curves over $\mathbb{Q}_p$ that acquire good reduction over extensions of degrees 2, 3, 4 and 6. In the next section, we shift our focus to elliptic curves defined over $\mathbb{Q}$. In this global setting, we will see that no elliptic curve defined over $\mathbb{Q}$ can achieve good reduction everywhere over quadratic extensions of $\mathbb{Q}$.

5.2 Good reduction everywhere over quadratic fields

Let $E/\mathbb{Q}$ be an elliptic curve, and let $K/\mathbb{Q}$ be a quadratic extension. In this section, we study the behavior of E over K, focusing on the possibility of acquiring good reduction everywhere. The main result is the following:

Theorem 5.3. *Let E be an elliptic curve over $\mathbb{Q}$. If K is a quadratic field, then the base change of E to K always has bad reduction at some prime ideal.*

In order to prove the theorem above, we need to introduce a few results. We begin by relating the conductors of E and its quadratic twist:

Proposition 5.4 (Kida)**.** *Let L/K be a quadratic extension of number fields and E an elliptic curve defined over K. Then*

$$N_{L/K}(\mathrm{Cond}(E_L)) \cdot (\Delta_{L/K})^2 = \mathrm{Cond}(E) \cdot \mathrm{Cond}(E^L)$$

where $\Delta_{L/K}$ is the relative discriminant of L/K and $N_{L/K}$ the norm map.

Proof. See Proposition 1.1 in [4]. □

Lemma 5.5. *Let E be an elliptic curve defined over $\mathbb{Q}_p$ and $L/\mathbb{Q}_p$ a quadratic extension, i.e., $L = \mathbb{Q}_p(\sqrt{d})$ with $d \in \mathbb{Z}_p$ squarefree. Let c_i and Δ be the corresponding quantities of a model of E, and c_i' and Δ', of the twist E^L. The following hold:*

$$v_p(c_i') = v_p(c_i) + i\frac{v_p(d)}{2}, \quad (i = 4, 6)$$

and

$$v_p(\Delta') = v_p(\Delta) + 6v_p(d).$$

Proof. Let η be such that $\eta^2 = \dfrac{1}{d}$. Then, we know from Example 4.18 that the quadratic twist by d of E is given by the coordinate change

$$x = \eta^2 x \qquad \text{and} \qquad y = \eta^3 y' + a_1(\eta - 1)u^2 x' + \frac{a_3(\eta^3 - 1)}{2},$$

which yields the Weierstrass equation for E^L,

$$y^2 + a_1xy + a_3y = x^3 + \left(a_2d + \frac{a_1^2(d-1)}{4}\right)x^2 + \left(a_4d^2 + \frac{a_1a_3(d^2-1)}{2}\right)x + \left(a_6d^3 + \frac{a_3^2(d^3-1)}{4}\right)$$

From the coordinate change table (Table 1), we have

$$\eta^i c_i' = c_i, \qquad \text{for } i = 4, 6$$

hence

$$v_p(\eta^i c_i') = v_p(c_i) \iff iv_p(\eta) + v_p(c_i') = v_p(c_i) \iff$$
$$v_p(c_i') = v_p(c_i) - iv_p(d^{-1/2}) \iff v_p(c_i') = v_p(c_i) + i\frac{v_p(d)}{2}.$$

Similarly, from the same table we have

$$\eta^{12}\Delta' = \Delta$$

so

$$v_p(\eta^{12}\Delta') = v_p(\Delta) \iff 12v_p(\eta) + v_p(\Delta') = v_p(\Delta) \iff$$
$$v_p(\Delta') = v_p(\Delta) - 12v_p(d^{-1/2}) \iff v_p(\Delta') = v_p(\Delta) - 6v_p(d),$$

hence we are done. □

Proposition 5.6. *Let $L/\mathbb{Q}_p$ be a ramified quadratic extension and E an elliptic curve defined over $\mathbb{Q}_p$ with minimal discriminant Δ. Then, the following are equivalent*

(i) The base change E_L has good reduction.

(ii) Either E or the quadratic twist E^L has good reduction.

Moreover, if the above hold, then the reduction type of E is one of the following:

$$\begin{aligned}
&\mathrm{Type}(E) = I_0 \quad \textit{or} \quad I_0^* && \textit{if } p \geqslant 3,\\
&\mathrm{Type}(E) = I_0 \\
&\qquad \textit{or} \quad II^* \quad \textit{with} \quad v_2(\Delta) = 12 \\
&\qquad \textit{or} \quad I_4^* \quad \textit{with} \quad v_2(\Delta) = 12 && \textit{if } p = 2 \textit{ and } v_2(\Delta_{L/\mathbb{Q}_2}) = 2\\
&\mathrm{Type}(E) = I_0 \\
&\qquad \textit{or} \quad II \quad \textit{with} \quad v_2(\Delta) = 6 \\
&\qquad \textit{or} \quad I_8^* \quad \textit{with} \quad v_2(\Delta) = 18 && \textit{if } p = 2 \textit{ and } v_2(\Delta_{L/\mathbb{Q}_2}) = 3
\end{aligned}$$

Proof. First, assume that either E or E^L has good reduction. Then, by the *Semistable reduction theorem* (4.32 (b)), either E_L or $(E^L)_L$ has good reduction respectively. But E_L and $(E^L)_L$ are isomorphic, hence E_L must have good reduction. This shows that *(ii)* follows from *(i)*.

Suppose now that E_L has good reduction. Then $\mathrm{Type}(E_L) = I_0$, and so we know that $\mathrm{Cond}(E_L)$ is trivial thus,

$$N_{L/K}(\mathrm{Cond}(E_L)) = (1)$$

hence the equality in Proposition 5.4 becomes

$$(\Delta_{L/\mathbb{Q}_p})^2 = \mathrm{Cond}(E) \cdot \mathrm{Cond}(E^L). \tag{10}$$

Now, assume that E has multiplicative reduction. The *Semistable reduction theorem* 4.32 (b), this implies that E_L must have multiplicative reduction as well. But this contradicts the assumption that E_L has good reduction, hence it is only possible that either E has additive or good reduction. Let us move our attention to the case where E has additive reduction.

From Section 3.4.2, we obtain that for $p \geqslant 3$ the discriminant of $L/\mathbb{Q}_p$ is given by p hence (10) becomes

$$p^2 = \mathrm{Cond}(E) \cdot \mathrm{Cond}(E^L). \tag{11}$$

Moreover, for $p \geqslant 5$, we also know from Table 2 that $\mathrm{Cond}(E) = p^2$ (as E must have additive reduction), so

$$p^2 = p^2 \,\mathrm{Cond}\, E^L \iff \mathrm{Cond}(E^L) = 1$$

showing that E^L has good reduction and thus proving *(ii)* for $p \geqslant 5$. Now, since E^L has good reduction over $\mathbb{Q}_p$, we have $v_p(\Delta') = 0$. But this holds under any change of coordinates

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + su^2x' + t, \qquad \text{with } u \in \mathbb{Q}_p^\times, r, s, t \in \mathbb{Q}_p$$

hence, the new discriminant also satisfies $v_p(u^{-12}\Delta) = 0$ for every such change of variables; therefore, it holds that

$$v_p(\Delta') \equiv 0 \pmod{12}$$

and, consequently, by Lemma 5.5, we need

$$v_p(\Delta) + 6v_p(d) = 0 \iff v(\Delta) \equiv 6 \pmod{12}$$

where we have used the fact that $v(d) = 1$ from Section 3.4.2. The minimality of Δ then implies that $v_p(\Delta) = 6$ since we must have $v_p(\Delta) < 12$ from Proposition 4.21. From Table 2 we then see that this is the case precisely when $\text{Type}(E) = I_0^*$.

Let now $p = 3$. Then, $2v_3(\Delta) \equiv 0 \pmod{12}$. To see this, let

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + su^2x' + t, \qquad \text{with } u \in O_L^\times \text{ and } r, s, t \in O_L$$

be the change of variables that produces a minimal equation of E over L and let $\tilde{\Delta}$ be its discriminant. Then

$$v_L(\tilde{\Delta}) = v_L(u^{-12}\Delta) = v_L(\Delta) - 12v_L(u) = v_L(\Delta).$$

Note that $e_{L/\mathbb{Q}_3} = v_L(3)$ and that L is a totally ramified extension of $\mathbb{Q}_3$. This follows from the fact that L is ramified, so $1 < e_{L/\mathbb{Q}_3} \leqslant [L : \mathbb{Q}_3] = 2$ therefore it must be that $e_{L/\mathbb{Q}_p} = [L : \mathbb{Q}_3]$, hence

$$v_L(\Delta) = 2v_3(\Delta)$$

and since by the same argument as above $v_L(\tilde{\Delta}) \equiv 0 \pmod{12}$, it must be that

$$2v_3(\Delta) \equiv 0 \pmod{12}.$$

Moreover, we must also have $v_3(\text{Cond}(E)) \leqslant 2$ from (11). Then from Table II in [8], there are only two possibilities, $\text{Type}(E) = I_0^*$ or $\text{Type}(E) = I_n^*$ with $n > 0$. If $\text{Type}(E) = I_n^*$, by Proposition 1 in [1], we have $\text{Type}(E^L) = I_n$, i.e., the twist E^L has multiplicative reduction, which implies that E_L has multiplicative reduction, a contradiction. Thus, we have again that $\text{Type}(E) = I_0^*$, so Proposition 1 in [1] implies that $\text{Type}(E^L) = I_0$ proving the proposition for $p = 3$.

Finally, we assume that $p = 2$. Let us firstly consider the case where $v_2(\Delta_{L/\mathbb{Q}_2}) = 2$. Then (10) yields

$$2^4 = \text{Cond}(E) \cdot \text{Cond}(E^L) \tag{12}$$

and thus, it is necessary that $v_2(\text{Cond}(E)) \leqslant 4$. Additionally, completely analogously as in the $p = 3$ case, we need to have $2v_2(\Delta) \equiv 0 \pmod{12}$ since L is totally ramified. From Table IV in [8] the above implies that we can only have $\text{Type}(E) = II^*$ with $v_2(\Delta) = 12$, or $\text{Type}(E) = I_n^*$ with $v_2(\Delta) = 8 + n$. Note that for the latter, $2v_2(\Delta) \equiv 0 \pmod{12}$ does not hold for all values of $n > 0$, hence we need that

$$2(n + 8) \equiv 0 \pmod{12} \iff 2n \equiv 8 \pmod{12} \iff n = 4 + 12k$$

Then, again Table IV from [8] implies

$$v_L(c_4) = 2 \cdot 4, \qquad v_L(\Delta) = 2 \cdot (12 + 12k) = 12 \cdot 2(1 + k).$$

Suppose that π is a prime element of L. Then, in order for E_L to have good reduction, we need precisely $2(k + 1)$ applications of the coordinate change

$$x = \pi^2x' + r \qquad \text{and} \qquad y = \pi^3y' + s\pi^2x' + t$$

in order to obtain

$$v_L(\Delta') = v_L(\pi^{-12\cdot 2(k+1)}\Delta) = 0$$

hence we also have

$$\begin{aligned} v_L(c_4') &= v_L(\pi^{-4\cdot 2(k+1)}c_4) = -8(k+1)+8 = -8k \geqslant 0 \\ v_L(c_6') &= v_L(\pi^{-6\cdot 2(k+1)}c_6) = -12(k+1)+12 = -12k \geqslant 0 \end{aligned}$$

where in the above we used Table 1 and that it is necessary that $c_4, c_6 \in \mathcal{O}_L$. Thus, we can only have $k = 0$, which implies that we can only have

$$\begin{aligned} \text{Type}(E) &= II^*, \qquad v_2(\Delta) = 12; \\ \text{Type}(E) &= I_4^*, \qquad v_2(\Delta) = 12. \end{aligned}$$

Both cases above satisfy $v_2(\text{Cond}(E)) = 4$, hence it must be that $v_2(\text{Cond}(E^L)) = 1$ from (12).

Assume now that $v_2(\Delta_{L/\mathbb{Q}_2}) = 3$. Then (10) gives

$$2^6 = \text{Cond}(E)\cdot\text{Cond}(E^L). \tag{13}$$

Then, $v_2(\text{Cond}(E)) \leqslant 6$ is needed. By imposing again the condition that $2v_2(\Delta) \equiv 0 \pmod{12}$ and looking the values up in Table IV from [8] we see that this condition holds only when $v_2(\text{Cond}(E)) \geqslant 4$. Then, using the aforementioned table, we can separate the type of E, depending on the valuation of its conductor.

I. $v_2(\text{Cond}(E)) = 4$
Here we only have two possibilities:

$$\begin{aligned} \text{Type}(E) = II^* \qquad &\text{with} \quad v_2(c_4) \geqslant 8, v_2(c_6) = 9, v_2(\Delta) = 12, \\ \text{Type}(E) = I_4^* \qquad &\text{with} \quad v_2(c_4) \geqslant 4, v_2(c_6) = 6, v_2(\Delta) = 12. \end{aligned}$$

Note that in both cases we have $\text{Cond}(E^L) = 2^2$.

Suppose first that $\text{Type}(E) = II^*$. Twisting then yields

$$\begin{aligned} v_2(c_4') &= v_2(c_4) + 2 \geqslant 10 \\ v_2(c_6') &= v_2(c_6) + 3 = 12 \\ v_2(\Delta') &= v_2(\Delta) + 6 = 18 \end{aligned}$$

by Lemma 5.5. From Table IV in [8] we also know that the equation is not minimal whenever $v_2(c_4) \geqslant 8$, $v_2(c_6) \geqslant 11$ and $v_2(\Delta) \geqslant 18$, the equation is not minimal. Consider the change of variables

$$x = \pi^2 x' + r \qquad \text{and} \qquad y = \pi^3 y' + s\pi^2 x' + t$$

as above with corresponding quantities c_4'', c_6'' and Δ''. The change of variables table (Table 1) then gives

$$\begin{aligned} v_2(c_4'') &= v_2(\pi^{-4}c_4') \geqslant -4+8 = 6, \\ v_2(c_6'') &= v_2(\pi^{-6}c_6') = -6+12 = 6, \\ v_2(\Delta'') &= v_2(\pi^{-12}\Delta) = -12+18 = 6, \end{aligned}$$

but looking this up in Table IV from [8] again we see that $\text{Type}(E^L) = II$ with $\text{Cond}(E^L) = 6$, a contradiction.

The only other option is then $\text{Type}(E) = I_4^*$. The quadratic twist gives

$$\begin{aligned} v_2(c_4') &= v_2(c_4) + 2 \geqslant 6 \\ v_2(c_6') &= v_2(c_6) + 3 \geqslant 9 \\ v_2(\Delta') &= v_2(\Delta) + 6 = 18 \end{aligned}$$

and from Table IV in [8] we see that the only possibility is that $\text{Type}(E^L) = I_8^*$ and hence we read that $\text{Cond}(E^L) = 6$, yet again, a contradiction. Therefore we cannot have that $v_2(\text{Cond}(E)) = 4$.

II. $v_2(\text{Cond}(E)) = 5$
From (13) we obtain $v_2(\text{Cond}(E^L)) = 1$, i.e., E^L has multiplicative reduction. Since $E_L \cong (E_L)^L$ over L, it must be that E_L has multiplicative reduction, but this contradicts our assumption that E_L has good reduction. Thus, $v_2(\text{Cond}(E^L)) \neq 5$.

III. $v_2(\text{Cond}(E)) = 6$
From above, we see that this is the only possible case and from (13) we have that $v_2(\text{Cond}(E^L)) = 0$, in other words, E^L has good reduction. Recall the condition

$$v_2(\Delta) \equiv 0 \pmod{12}.$$

Using the above and Table IV from [8] we see that the reduction types of E are

$$\begin{aligned} \text{Type}(E) &= II, \qquad \text{with} \quad v_2(\Delta) = 6, \\ \text{Type}(E) &= I_8^*, \qquad \text{with} \quad v_2(\Delta) = 18, \\ \text{Type}(E) &= I_2^*, \qquad \text{with} \quad v_2(\Delta) = 12. \end{aligned}$$

We shall prove that the last case is impossible. Since $v_2(\Delta_{L/\mathbb{Q}_2}) = 3$, take $L = \mathbb{Q}_2(\sqrt{d})$ with $v_2(d) = 1$. Then, by Lemma 5.5

$$v_2(\Delta') = v_2(\Delta) + 6 = 18,$$

but $18 \not\equiv 0 \pmod{12}$, hence E^L does not have good reduction in this case. This completes the proof for $p = 2$, hence the proof of the theorem.

□

Now that we have all the necessary tools, we are able to prove Theorem 5.3.

Proof. Consider an elliptic curve E defined over $\mathbb{Q}$. Suppose that E has good reduction at every finite prime of some quadratic extension K. Then it must be that E satisfies all of the requirements of Proposition 5.6 for all primes. Let S be the set of primes at which E has bad reduction over $\mathbb{Q}_p$. That is, define

$$S = \{p | \, \text{Type}(E, p) \neq I_0\}.$$

Furthermore, define a quadratic field L over $\mathbb{Q}$ as follows. If $2 \notin S$, set $m = \prod_{p \in S} p$ and

$$\begin{aligned} L &= \mathbb{Q}(\sqrt{m}) \qquad \text{if } m \equiv 1 \pmod 4 \\ L &= \mathbb{Q}(\sqrt{-m}) \qquad \text{if } m \equiv 3 \pmod 4. \end{aligned}$$

For $2 \in S$, set $m = (\prod_{p \in S} p)/2$ and

$$\begin{aligned}
&L = \mathbb{Q}(\sqrt{\pm 2m}) && \text{if} \quad \text{Type}(E,2) = II \text{ or } I_8^*, \\
&L = \mathbb{Q}(\sqrt{m}) && \text{if} \quad \text{Type}(E,2) = II^* \text{ or } I_4^* \quad \text{and} \quad \text{if } m \equiv 3 \pmod 4, \\
&L = \mathbb{Q}(\sqrt{-m}) && \text{if} \quad \text{Type}(E,2) = II^* \text{ or } I_4^* \quad \text{and} \quad \text{if } m \equiv 1 \pmod 4,
\end{aligned}$$

where the sign of $2m$ is chosen such that the quadratic twist E^L has good reduction at 2. We construct L in this way such that only the primes of bad reduction ramify. Indeed, if $2 \notin S$, for both $m \equiv 1 \pmod 4$ and $m \equiv 3 \pmod 4$, we have $\Delta_{L/\mathbb{Q}} = m$. In the case that 2 is a bad prime we also constructed L, depending on the type of reduction E can have. If $\text{Type}(E, 2) = II$ or I_8^*, we need $v_2(\Delta_{L/\mathbb{Q}}) = 3$ from the previous proposition, so we choose $L = \mathbb{Q}(\sqrt{\pm 2m})$ so that $m \equiv 2 \pmod 4$, which gives $\Delta_{L/\mathbb{Q}} = \pm 4 \cdot 2m$. In the case that $\text{Type}(E, 2) = II^*$ or I_4^*, we need that $v_2(\Delta_L/\mathbb{Q}) = 2$ hence we put L as above depending on the value of m such that $\Delta_{L/\mathbb{Q}} = 4m$. Now, we are able to comfortably use Proposition 5.6.

Consider the quadratic twist E^L of E. If some prime number $p \in S$, then by Proposition 5.6 (ii), we have $\text{Type}(E^L, p) = I_0$, hence $v_p(\text{Cond}(E^L)) = 0$. If $p \notin S$, by Proposition 5.4:

$$\begin{aligned}
v_p(N_{L/\mathbb{Q}}(\text{Cond}(E_L)) \cdot \Delta_{L/\mathbb{Q}}) &= v_p(\text{Cond}(E) \cdot \text{Cond}(E^L)) \\
v_p(N_{L/\mathbb{Q}}) + v_p(\Delta_{L/\mathbb{Q}}) &= v_p(\text{Cond}\, E) + v_p(\text{Cond}\, E^L) \\
0 + 0 &= 0 + v_p(\text{Cond}(E^L))
\end{aligned}$$

hence $v_p(\text{Cond}(E^L)) = 0$. Therefore, the twist E^L is an elliptic curve defined over $\mathbb{Q}$ with good reduction everywhere. However, this contradicts Tate's result [7] which states that there exists no such curve.

□

5.3 Examples: Good reduction everywhere

In this section, we look at some elliptic curves that achieve good reduction everywhere over number fields of degrees $3, 4, 6$ and 12.

5.3.1 Cubic fields

Consider the elliptic $E/\mathbb{Q}$ curve given by the Weierstrass equation

$$E : y^2 + xy = x^3 + x^2 - 2x - 7.$$

This is a minimal equation. Indeed, $\Delta = -11^4$, so $v_{11}(\Delta) = 4 < 12$ and all coefficients are in the ring of integers $\mathbb{Z}_{11}$.
Since the discriminant of the above curve is given by $\Delta = -14641 = -11^4$, the curve has bad reduction at $p = 11$. In particular, we have

$$c_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3) = 25 - 24 \cdot (-4) = 121 = 11^2,$$

so $v_{11}(\Delta) = 4$ and $v_{11}(c_4) = 2$, that is, the reduction is additive. Looking for these values in Table 2 we find $\text{Type}(E/\mathbb{Q}, 11) = IV$.

This curve attains good reduction over the cubic field $\mathbb{Q}(\sqrt[3]{11})$. To see this, consider the change of variables

$$x = \sqrt[3]{11^2}x' + 6 \qquad \text{and} \qquad y = 11y' + 5\sqrt[3]{11^2}x' + 8$$

which gives the equation

$$y^2 + \sqrt[3]{11^2}xy + 2y = x^3 - \sqrt[3]{11}x^2 + 1$$

over $\mathbb{Q}(\sqrt[3]{11})$. The resulting equation has discriminant $\Delta' = -1$ and all coefficients are in $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{11})} = \mathbb{Z}(\sqrt[3]{11})$. Therefore, the equation is minimal and, moreover, since $\Delta' = -1$, it has good reduction everywhere.

5.3.2 Quartic Fields

The elliptic curve

$$E : y^2 + xy = x^3 - x^2 - 2x - 1$$

defined over $\mathbb{Q}$ with discriminant $\Delta = -343 = -7^3$ has good reduction everywhere except at $p = 7$. In order to determine the type of bad reduction at 7, compute

$$c_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3) = 9 + 24 \cdot 4 = 105 = 3 \cdot 5 \cdot 7$$

hence $v_7(c_4) = 1 > 0$. Moreover, we have $v_7(\Delta) = 3 > 0$, thus we have additive reduction. Looking up these values in Table 2, we see that $\text{Type}(E,\ 7) = III$.

Consider the change of coordinates (5) with $u = \sqrt[4]{7}, r = -12, s = 3, t = 6$. This gives new curve over $\mathbb{Q}(\sqrt[4]{7})$

$$E' : y^2 + \sqrt[4]{7^2}xy + 2y = x^3 - \sqrt[4]{7}x^2 + 1$$

that has good reduction everywhere. Indeed, we have that $\mathcal{O}_{\mathbb{Q}(\sqrt[4]{7})} = \mathbb{Z}[\sqrt[4]{7}]$, hence it is clear that all coefficients of E' lie in the ring of integers. Furthermore, the discriminant of E' is $\Delta' = -1$, which shows that not only the equation is minimal, but also that there are no bad primes for this curve.

Remark 5.7. *In this case,* 4 *is the minimal degree of an extension over which E acquires good reduction. The only smaller possibility is a quadratic extension, but we have already shown that this is insufficient. Therefore, no extension of smaller degree than* 4 *can eliminate the bad reduction of E, and the quartic field is minimal.*

5.3.3 Sextic Fields

The elliptic curve

$$E : y^2 + xy + y = x^3 + x^2 - 30x - 76$$

over the rational field $\mathbb{Q}$ with discriminant $\Delta = -11^2$ has additive reduction at $p = 11$ with $\text{Type}(E,\ 11) = II$. To see this, we find

$$c_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3) = 25 - 24(-60 + 1) = 1441 = 7 \cdot 131$$

which gives $v_{11}(c_4) = 1$, and we also have $v_{11}(\Delta) = 2$. Looking up Table 2, we indeed see that Type$(E, 11) = II$.

Through the change of coordinates

$$x = \sqrt[6]{11^2}x' + 6 \qquad \text{and} \qquad y = \sqrt[6]{11^3}y' + 5\sqrt[6]{11^2}x' + 2$$

we obtain the equation

$$E' : y^2 + \sqrt[6]{11^5}xy + \sqrt{11}y = x^3 - \sqrt[6]{11^4}x^2 + 3\sqrt[3]{11}x - 2.$$

with all the coefficients in $\mathcal{O}_{\mathbb{Q}(\sqrt[6]{11})} = \mathbb{Z}(\sqrt[6]{11})$ and discriminant $\Delta' = -1 < 12$, hence minimal. Moreover, since $\Delta' = -1$ the new curve has good reduction everywhere over $\mathbb{Q}(\sqrt[6]{11})$.

Remark 5.8. *In this case,* 6 *is indeed the minimal degree of an extension such that E acquires good reduction. The only smaller degree we could have is* 3*, but this is impossible. To see this, suppose we want to eliminate the bad reduction at* $p = 11$ *by passing to a cubic extension* $K/\mathbb{Q}$ *and denote the discriminant of the base change curve by* Δ'*. By the Semistable reduction theorem (Proposition 4.32) we need* 11 *to ramify in K. There are two possible factorizations of* 11 *in* $\mathcal{O}_K$*:*

$$11\mathcal{O}_K = \mathfrak{P}_1^2\mathfrak{P}_2 \qquad \textit{or} \qquad 11\mathcal{O}_K = \mathfrak{P}^3.$$

Let us consider the first case. Since $v_{11}(\Delta) = 2$*, the base change of the elliptic curve to K gives:*

$$v_{\mathfrak{P}_g}(\Delta') = 2v_{11}(\Delta) = 4 \qquad \textit{and} \qquad v_{\mathfrak{P}_y}(\Delta') = v_{11}(\Delta) = 2.$$

Now, since we assumed that we can get rid of the bad reduction at 11 *over K, there exists a change of variables such in 4.23 (b) such that*

$$v_{\mathfrak{P}_1}(\Delta') - 12v_{\mathfrak{P}_1}(u) = v_{\mathfrak{P}_2}(\Delta') - 12v_{\mathfrak{P}_2}(u) = 0.$$

That is, we need

$$v_{\mathfrak{P}_1}(u) = \frac{1}{3} \qquad \textit{and} \qquad v_{\mathfrak{P}_2}(u) = \frac{1}{6}$$

which is clearly impossible as the image of discrete valuations must in $\mathbb{Z}$ *by definition. Therefore, the only remaining possibility is that* $11\mathcal{O}_K = \mathfrak{P}^3$*. We have*

$$v_{\mathfrak{P}}(\Delta') = 3v_{\mathfrak{P}}(\Delta) = 6,$$

and we need some $u \in \mathcal{O}_K$ *such that*

$$v_{\mathfrak{P}}(\Delta') - 12v_{\mathfrak{P}}(u) = 0 \iff v_{\mathfrak{P}}(u) = \frac{1}{6},$$

which is again, impossible.

This shows that E cannot possibly attain good reduction everywhere over any cubic extension of $\mathbb{Q}$*.*

References

[1] S. Comalada, "Twists and reduction of an elliptic curve," *Journal of Number Theory*, vol. 49, no. 1, pp. 45–62, 1994, ISSN: 0022-314X. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022314X84710791.

[2] F. Gouvêa, *p-adic Numbers: An Introduction* (Universitext). Springer International Publishing, 2020, ISBN: 9783030472955. [Online]. Available: https://books.google.nl/books?id=VWjsDwAAQBAJ.

[3] G. Janusz, *Algebraic Number Fields* (Advances in the Mathematical Sciences). American Mathematical Society, 1996, ISBN: 9780821804292. [Online]. Available: https://books.google.nl/books?id=rw0PCgAAQBAJ.

[4] M. Kida, "Potential good reduction of elliptic curves," *Journal of Symbolic Computation*, vol. 34, no. 3, pp. 173–180, 2002, ISSN: 0747-7171. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747717102905559.

[5] Á. Lozano-Robledo, "Ramification in the division fields of elliptic curves with potential supersingular reduction," *Research in Number Theory*, vol. 2, no. 1, p. 8, 2016. [Online]. Available: https://link.springer.com/article/10.1007/s40993-016-0040-z.

[6] J. Neukirch and N. Schappacher, *Algebraic Number Theory* (Grundlehren der mathematischen Wissenschaften). Springer Berlin Heidelberg, 2013, ISBN: 9783662039830. [Online]. Available: https://books.google.nl/books?id=hS3qCAAAQBAJ.

[7] A. P. Ogg, "Abelian curves of 2-power conductor," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 62, no. 2, pp. 143–148, 1966. DOI: 10.1017/S0305004100039670.

[8] I. Papadopoulos, "Neron classification of elliptic curves where the residual characteristics equal 2 or 3," *Journal of Number Theory*, vol. 44, no. 2, pp. 119–152, 1993, ISSN: 0022-314X. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022314X83710401.

[9] A. Robert, *A Course in p-adic Analysis* (Graduate Texts in Mathematics). Springer New York, 2000, ISBN: 9780387986692. [Online]. Available: https://books.google.nl/books?id=H6sq_x2-DgoC.

[10] J. Serre and M. Greenberg, *Local Fields* (Graduate Texts in Mathematics). Springer New York, 2013, ISBN: 9781475756739. [Online]. Available: https://books.google.nl/books?id=3LAJCAAAQBAJ.

[11] J. Silverman, *The Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics). Springer New York, 2009, ISBN: 9780387094946. [Online]. Available: https://books.google.nl/books?id=Z90CA_EUCCkC.

[12] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* (Graduate Texts in Mathematics). Springer New York, 2013, ISBN: 9781461208518. [Online]. Available: https://books.google.nl/books?id=VIJ3BQAAQBAJ.