RECIPROCITY LAWS

Gaurish Korpal[1]
gaurish.korpal@niser.ac.in

Winter Internship Project Report

[1]3^{rd} year Int. MSc. Student, National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha)

Certificate

Certified that the winter internship project report "Reciprocity Laws" is the bona fide work of "Gaurish Korpal", 3^{rd} Year Int. MSc. student at National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha), carried out under my supervision during December 09, 2016 to January 07, 2017.

Place: Allahabad
Date: January 07, 2017

Prof. Chandan Singh Dalawat
Supervisor
Professor H+,
Harish-Chandra Research Institute,
Jhusi, Allahabad 211091

Abstract

In this report, the meaning of reciprocity laws and Hilbert's formulation of local quadratic reciprocity law have been discussed. Using this formulation, Hilbert was able to state and prove a form of quadratic reciprocity over any number field, in which the corresponding product of symbols is quantified over the prime ideals of the number field. This led to a proper understanding of what we today call "classical reciprocity laws".

Acknowledgements

This report would not have existed in this neat-to-read form without the access to awesome typesetting tools. I would like to thank the people who created these tools and made them available for free for everyone.

- Donald Knuth for TeX
- Michael Spivak for $\mathcal{AMS}$-TeX
- Sebastian Rahtz for TeX Live
- Leslie Lamport for LaTeX
- American Mathematical Society for $\mathcal{AMS}$-LaTeX
- Hàn Thế Thành for pdfTeX
  - Christian Feuersänger & Till Tantau for PGF/TikZ interpreter
  - Heiko Oberdiek for hyperref package
  - Steven B. Segletes for stackengine package
  - Michael Shell for ieeetrantools package
  - Alan Jeffrey & Frank Mittelbach for inputenc package
  - David Carlisle for graphicx package
  - Javier Bezos for enumitem package
  - Hideo Umeki for geometry package
  - Axel Sommerfeldt for subcaption package
  - Philipp Lehman & Joseph Wright for csquotes package
  - Jerry Leichter & Piet van Oostrum for multirow package
  - David Carlisle & David Kastrup for longtable package
- Philipp Kühl & Daniel Kirsch for Detexify (a tool for searching LaTeX symbols)
- TeX.StackExchange community for helping me out with LaTeX related problems

Contents

Introduction

Reciprocity Laws form the backbone of what we call "global number theory". On the other hand, modular arithmetic marks the beginnings of what we call "local number theory". In words of Barry Mazur (from foreword of [4])

> A local problem is one which concerns itself with issues regarding divisibility by a single prime number p, or by its powers. Global problems, in contrast, constitute the basic hard questions we wish to answer about whole numbers. Reciprocity laws, when available, represent the extra glue, the further constraint, in a problem of global number theory that ties together all corresponding problems in various local number theories connected to each of the prime numbers $p = 2, 3, 5, 7, \ldots$

The term *reciprocity* was first used by Adrien-Marie Legendre[1] to emphasize that "if p and q are distinct odd primes and at least one of them is $\equiv 1 \pmod 4$ then q is a square modulo p if and only if p is a square modulo q"[14]. This statement is part of following:

Theorem (Quadratic reciprocity law)**.** *Let p and q be distinct odd primes, then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad ; \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad ; \quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

where, for any co-prime integers u and v we define $\left(\frac{u}{v}\right) = 1$ if u is a square modulo v and $\left(\frac{u}{v}\right) = -1$ otherwise and is called Legendre symbol.

This theorem was first proved by Carl Friedrich Gauss in 1801, and today many proofs are known. For example, I have discussed two of the ways to prove it in my previous reports [15, 16]. This theorem may appear to violate our intuition that congruences modulo different primes should act independently, but its need arises naturally while solving Diophantine equations [15] and representing numbers as sum of squares [12].

Once the *quadratic reciprocity law* was well established, it was natural to try to extend this notion of *reciprocity* to higher powers modulo p. For example, we can define *quartic reciprocity law* using the ring of *Gaussian integers*[15] as:

Theorem (Quartic reciprocity law)**.** *Let $a + b\iota$ and $c + d\iota$ be distinct Gaussian primes congruent to 1 modulo $2 + 2\iota$, then*

$$\left(\frac{\iota}{a+b\iota}\right)_4 = (-1)^{\frac{1-a}{4}} \quad ; \quad \left(\frac{1+\iota}{a+b\iota}\right)_4 = (-1)^{\frac{a-b-1-b^2}{8}} \quad ; \quad \left(\frac{c+d\iota}{a+b\iota}\right)_4\left(\frac{a+b\iota}{c+d\iota}\right)_4 = (-1)^{\frac{a^2+b^2-1}{4}\cdot\frac{c^2+d^2-1}{4}}$$

where, for any Gaussian integer $s + t\iota$ not divisible by $u + v\iota$ we define $\left(\frac{s+t\iota}{u+v\iota}\right)_4 = 1$ if $s + t\iota$ is a fourth-power modulo $u + v\iota$ and $\left(\frac{s+t\iota}{u+v\iota}\right)_4 = -1$ otherwise.

This theorem was first proved by Gotthold Eisenstein in 1844, for details one may refer to the book by Franz Lemmermeyer[2]. But, in this report we won't see proofs of any particular reciprocity law, rather will focus on building theory towards the generalized reciprocity law.

[1] A. M. Legendre, *Essai sur la Théorie des Nombres*, Paris, 1797. par. 164

[2] Reciprocity Laws: from Euler to Eisenstein. Berlin: Springer (2000).

Chapter 1

Reciprocity Ideas

Having observed the existence of various reciprocity laws, we must carefully look at the meaning of this term. According to Wyman[11]

> Suppose $f(X)$ is a monic irreducible polynomial with integral coefficients, and suppose p is a prime number. Reducing the coefficients of $f(X)$ modulo p gives a polynomial $f_p(X)$ with coefficients in the field $\mathbb{F}_p$ of p elements. The polynomial $f_p(X)$ may factor (even though the original $f(X)$ was irreducible). If $f_p(X)$ factors over $\mathbb{F}_p$ into a product of distinct linear factors, we say that $f(X)$ splits completely modulo p, and we define $\mathrm{Spl}(f)$ to be the set of all primes such that $f(X)$ splits completely modulo p. The general reciprocity problem we shall be considering is: *Given $f(X)$ as above, describe the factorization of $f_p(X)$ as a function of the prime p.* Sometimes we ask for less: *give a rule to determine which primes belong to* $\mathrm{Spl}(f)$. This vague question is hard to make precise until it is answered. What is a "rule"? What is an acceptable method for describing the factorization of $f(X)$? Anyway, a satisfactory answer to this unsatisfactory question will be called a *reciprocity law*.

To illustrate this interpretation, let's use *Chinese Remainder Theorem*

> Given integers a_i and n_i for $1 \leq i \leq k$. If $x \equiv a_i \pmod{n_i}$ for all i, then $x \equiv \sum_{i=1}^{k} a_i c_i d_i \pmod{n}$ where $n = \prod_{i=1}^{k} n_i$, $c_i = \frac{n}{n_i}$ and $c_i d_i \equiv 1 \pmod{n_i}$.

to re-state *quadratic reciprocity law* as:

Theorem (Quadratic reciprocity law)**.** *Suppose that q is an odd prime. Then the set $\mathrm{Spl}(x^2 - q)$ can be defined by congruence conditions modulo q if $q \equiv 1 \pmod 4$ and modulo $4q$ if $q \equiv 3 \pmod 4$. Furthermore, $\mathrm{Spl}(X^2 - 2)$ can be described by congruence conditions modulo 8.*

Therefore, quadratic reciprocity law gives a relationship between the solutions to $x^2 = q$ in $\mathbb{F}_p$ and $x^2 = p$ in $\mathbb{F}_q$, where p and q are two different odd primes[1]. This yields a nice description of sets $\mathrm{Spl}(f)$ for quadratic polynomials. We can find such a reciprocity law for certain special polynomials of higher degree, for example, for cyclotomic polynomials (I defined them in previous report [16]) :

[1] We can re-state this in terms of *algebraic variety* by using following defintion of *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if} \quad |S(\mathbb{F}_p)| = 0 \\ 0 & \text{if} \quad |S(\mathbb{F}_p)| = 1 \\ 1 & \text{if} \quad |S(\mathbb{F}_p)| = 2 \end{cases}$$

where $S := x^2 + 1$ is the algebraic variety and $S(\mathbb{F}_p)$ is the set of solutions of this variety (which is a single equation in this case) in $\mathbb{F}_p$ for some odd prime p. For more details refer Chapter 7 of [4]

Theorem (Cyclotomic reciprocity law)**.** *The cyclotomic polynomial $\Phi_m(X)$ factors into distinct linear factors modulo p if and only if $p \equiv 1 \pmod{n}$.*

For proof of this theorem one can refer to §3 of [11].

1.1 Frobenius

Ferdinand Georg Frobenius invented the method of using *characters* to study group representations. Linear representations of Galois groups allow us to generalize quadratic reciprocity into a vast theory of generalized reciprocity laws. *Characters* are the functions attached to linear representations of groups and have no exclusive relationship to number theory. In fact, they can be defined for any matrix representation of any group. But in number theory, the character has a special interpretation in context of reciprocity laws. I shall discuss them in future reports, but one can refer Chapter 15 in [4] for an exposition.

On the other hand, *Frobenius elements* belong to Galois groups and belong exclusively to number theory[4]. The Frobenius elements are defined for extensions L/K of *global fields* that are finite Galois extensions for prime ideals $\mathfrak{P}$ of L that are unramified in L/K. This was discussed in Theorem 22 on pp. 39 in [16], and I will say a bit more about them here. Firstly, let's look at following definitions.

Definition 1 (Frobenius endomorphism)**.** Let R be a commutative ring with prime characteristic p. The Frobenius endomorphism $F : R \to R$ is defined by $F(r) = r^p$ for all $r \in R$.

Note that F is a ring homomorphism since $F(rs) = F(r)F(s)$ and $F(r+s) = F(r) + F(s)$ (because in characteristic p ring $(r+s)^p = r^p + s^p$. Whenever this endomorphism is invertible we get an automorphism of R.

Definition 2 (Frobenius automorphism)**.** Let Γ be a finite extension of $\mathbb{F}_p$ with $[\Gamma : \mathbb{F}_p] = d$. The mapping $\psi : \Gamma \to \Gamma$ such that $\psi(z) = z^p$ and $\psi(z) = z$ if and only if $z \in \mathbb{F}_p$ is called Frobenius automorphism on Γ.

Note that, $\psi^i(z) = z$ for $1 \leq i \leq d$ if and only if $z \in \mathbb{F}_q \subset \Gamma$, where $q = p^i$. Thus d can be computed as the smallest integer such that ψ^d is an identity map on Γ. In general, the Galois group of an extension of an estension of finite fields is generated by an iterate of the Frobenius automorphism.

Suppose that τ is a matrix representation of the *absolute Galois group* G consisting of all permutations σ of field of algebraic integers $\mathbb{Q}^{\text{alg}}$ that preserve addition and multiplication. If for some field $\mathbb{F}$ we have $\tau : G \to \mathrm{GL}(n, \mathbb{F})$, then $\chi_\tau : G \to \mathbb{F}$ is the *character function*, with $\chi_\tau(\sigma) = \mathrm{trace}(\tau(\sigma))$ for any $\sigma \in G$. Let's denote[2] the Frobenius element of G by Frob_p where p is a prime integer. This Galois representation τ comes with a set S of *ramified primes* (see Definition 17 on pp. 36 of [16]), and if p is not in S i.e. τ is unramified at p, then $\chi_\tau(\mathrm{Frob}_p)$ is well defined. Moreover, we can only define $\mathrm{Frob}_p(\alpha)$ if p is unramified with respect to the algebraic integer α.

> For some examples of computing Frobenius elements, refer Chapter 16, pp. 185–186 of [4].

Note that, if $f(X) \in \mathbb{Z}[X]$ is a irreducible monic polynomial of degree n and p in unramified with respect to any of the roots of $f(X)$ then Frob_p permutes the roots of $f(X)$. We have following theorem which establishes a relationship between the *cycle* types of the permutations on the roots by Frob_p and $f_p(X)$ (for motivation and examples, refer pp. 186–189 of [4]).

[2] I am using a difffent notation from what I used in Definition 27 on pp. 39 of [16] since here I have given a more specific definition of Frobenius automorphism.

Theorem. *Suppose $f(X) \in \mathbb{Z}[X]$ is an irreducible polynomial and p is a prime not dividing the discriminant*[3] *of $f(X)$. If $f_p(X)$ factors into r factors, and the degrees of those r factors are $d_1, d_2, \ldots, d_r$, then the cycle type of Frob_p is $d_1 + d_2 + \ldots + d_r$ i.e. the integers d_i for $1 \leq i \leq r$ are the lengths of the cycles produced by the permutation on the roots.*

According to Ash & Gross[4] (restated in-terms of the notations introduced above):

> ...list of numbers $\chi_\tau(\mathrm{Frob}_2), \chi_\tau(\mathrm{Frob}_3), \chi_\tau(\mathrm{Frob}_5), \ldots$ (omitting from our list those p where τ is ramified, in which case $\chi_\tau(\mathrm{Frob}_p)$ is not really defined), is always a very interesting list of numbers. The whole idea of reciprocity laws is to try to find other independent ways of generating these lists of numbers. If we succeed, we obtain a type of theorem called a generalized reciprocity law, or simply a reciprocity law for short. ...
>
> ... a reciprocity law is a black box. You put in a prime p (where τ is unramified) and out pops a number. ...
>
> ... The equality between the traces of the matrices in a Galois representation and numbers produced by some sort of black box is what is called a reciprocity law. ...

We can think of the "independent way of generating $\chi_\tau(\mathrm{Frob}_p)$" as an input-output box, which Ash & Gross call "black box", having a label of "Reciprocity Law". We know *what* this box does to the input, but don't understand *why* it works. We can represent this idea pictorially as:

Moreover, these "black boxes" can be different types like some modular forms, some cohomology classes, etc. and I shall discuss them in future reports. For some concrete examples based on this idea of reciprocity laws refer Part Three, pp. 193–264 of [4].

1.2 Berlekamp's Algorithm

For a fixed $f(X)$ and a particular prime p, we can at least ask whether p lies in $\mathrm{Spl}(f)$. This involves factoring $f(X)$ modulo p, which is a finite process. I pointed towards the usage of *Berlekamp's algorithm* to factorize polynomials modulo p in my recent report ([16]; Example 2, pp. 55). We will have a look at a variant of this algorithm by Wyman[11].

Suppose we are given a polynomial $f(X) \in \mathbb{Z}[X]$ of degree n with no repeated factors. Let $f_p(X)$ be its reduction modulo p where p is a prime integer. If $f_p(X) = g_1(X)g_2(X)\cdots g_r(X)$ where $g_i(X)$ is irreducible polynomial of degree d_i with $\sum_{i=1}^{r} d_i = n$, our motive is to compute d_i so that we can classify the primes in $\mathrm{Spl}(f)$ based on the type of irreducible factors we get modulo p. To achieve this will use the ring-theoretic formulation of *Chinese Remainder Theorem*

> Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be pairwise relatively prime ideals in a ring R. The the mapping
>
> $$R \Big/ \bigcap_{i=1}^{n} \mathfrak{a}_i \mapsto R/\mathfrak{a}_1 \times \cdots R/\mathfrak{a}_n$$
>
> is an isomorphism. (pp. 253, [3])

[3] This ensures that p is unramified with respect to any of the roots of $f(X)$ following the Remark 18 on pp. 37 of [16]

along with the fact that since $g_i(X)$ is irreducible of degree d_i, the field $\mathbb{F}_p[X]/(g_i(X)) = \mathbb{F}_q$ is the unique finite field with $q = p^{d_i}$ elements. Also note that, $\mathbb{F}_p[X]/(f_p(X))$ is $n-$dimensional $\mathbb{F}_p$ space with basis $\{1, x, \ldots, x^{n-1}\}$ where x is the residue class of X modulo $f(X)$. Addition is vector space addition, and multiplication is carried out modulo $f(X)$. Following theorem, relatable to the theorem stated in previous section, is the backbone of the algorithm

Theorem. *Suppose it is given that*

$$\mathbb{F}_p[X]/(f_p(X)) = \mathbb{F}_p[X]/(g_1(X)) \oplus \cdots \oplus \mathbb{F}_p[X]/(g_r(X))$$

with $d_i = [\mathbb{F}_p[X]/(g_i(X)) : \mathbb{F}_p]$. *Let* ψ *be the Frobenius automorphism on* $\mathbb{F}_p[X]/(f_p(X))$. *If* ν_i *is the nullity*[4] *of the linear transformation*

$$(\psi^i - \mathrm{id}) : \mathbb{F}_p[X]/(f_p(X)) \to \mathbb{F}_p[X]/(f_p(X))$$

where $\mathrm{id} : \mathbb{F}_p[X]/(f_p(X)) \to \mathbb{F}_p[X]/(f_p(X))$ *is the identity map and* γ_j *is the number of factors in the given decomposition of* $\mathbb{F}_p[X]/(f_p(X))$ *which have dimension exactly equal to* j. *Then* $r = \nu_1$, *and there are exactly* γ_j *summands given by*

$$\gamma_j = \sum_{k=1}^{\lfloor \frac{n}{j} \rfloor} \sum_{m|jk} \frac{\mu(k)\mu(m)}{\phi(jk)} \nu_{\frac{jk}{m}}$$

where ϕ *and* μ *are the Euler and Möbius functions. Hence,* $d_i = j$ *for* $j = 1, 2, \ldots, d$ *where* d *is the smallest integer such that* $\psi^d = \mathrm{id}$.

Finally, here is the algorithm:

Step 1. Compute the discriminant of $f(X)$, $D(f)$.

Step 2. For prime $p \nmid D(f)$, compute the matrix $[\psi]$ with respect to the basis $\{1, x, \ldots, x^{n-1}\}$ of $\mathbb{F}_p[X]/(f_p(X))$.

Step 3. Compute successively $\nu_i = \mathrm{nullity}([\psi]^i - [\mathrm{id}])$.

Step 4. Compute γ_j from the theorem.

Remark 1. It's easy to compute discriminant of a polynomial if we know its roots (see, Remark 5 on pp. 14 of [16]), since we have:

$$D(f) = a_n^{2n-2} \prod_{1 \le i < j \le n} (r_i - r_j)^2$$

where $f(X) = \sum_{k=0}^{n} a_k X^k$ has complex roots r_i, $1 \le i \le n$. Moreover, we *define* a product with no factors to be equal to 1 (as in case of constant and linear polynomial).

But, computing the discriminant in Step 1. of a polynomial of degree n whose roots are unknown is in itself a difficult task. I know discriminant formula for following cases of $f(X) \in \mathbb{Z}[X]$

[4] It is the dimension of the kernel of the linear transformation involved. Here, $\nu_i = \dim_{\mathbb{F}_p}(\ker(\psi^i - \mathrm{id}))$. In fact, Lawrence J. Dickson derived the formula for ν_i in terms of γ_j:

$$\nu_i = \sum_{k=1}^{n} \gcd(k, m)\gamma_k$$

- If $f(X) = a_0 \neq 0$ then $D(f) = \frac{1}{a_0^2}$. (follows from the definition)
- If $f(X) = a_1X + a_0$ then $D(f) = 1$. (follows from the definition)
- If $f(X) = a_2X^2 + a_1X + a_0$ then $D(f) = a_1^2 - 4a_2a_0$. (by completing the squares method)
- If $f(X) = X^3 + a_1X + a_0$ then $D(f) = -(4a_1^3 + 27a_0^2)$. (exercise 28 on pp. 46 in [3]
- If $f(X) = X^5 + a_1X + a_0$ then $D(f) = 4^4a_1^5 + 5^5a_0^4$. (exercise 43 on pp. 52 in [3]; if coefficients are rational numbers then it is called *quintic in Bring-Jerrard form*)
- If $f(X) = X^5 + a_4X^4 + a_0$ then $D(f) = a_0^3(4^4a_4^5 + 5^5a_0^4)$. (exercise 44 on pp. 52 in [3])
- If $f(X) = X^3 + a_2X^2 + a_1X + a_0$ then $D(f) = a_2^2a_1^2 - 4a_1^3 - 4a_2^3a_0 - 27a_0^2 + 18a_2a_1a_0$. (exercise 48 on pp. 54 in [3])

To learn the general method for computing discriminants, refer exercise 45–47 on pp. 53–54 of [3] and §6.6 in [5]. ◊

Remark 2. In Step 2. we exclude the prime integer p which divides $D(f)$ from our discussion that follows. This is because $f_p(X)$ will have repeated factors (by Remark 18 on pp. 37 of [16]) and hence such p can't belong to $\mathrm{Spl}(f)$. ◊

Remark 3. In Step 3. we need to compute nullity. This may be done by appropriate column operations on the matrix $[\psi]^i - [\mathrm{id}]$, read §2.5 and §2.6 in [5]. Each such row vector in the null space of $[\psi]^i - [\mathrm{id}]$ represents a polynomial $g(x)$ which satisfies the equation $\{g(x)\}^p - g(x) \equiv 0 \pmod{f}(x)$, and, conversely, each $g(x)$ which satisfies this equation is represented by a row vector in the null space of $[\psi]^i - [\mathrm{id}]$. ◊

Remark 4. Both the Euler and Möbius function are arithmetic functions, i.e. functions from $\mathbb{N}$ to $\mathbb{C}$. Euler function counts the positive integers up to a given integer n that are relatively prime to n and can be written as

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Möbius function is defined as

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has one or more repeated prime factors} \\ 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \end{cases}$$

Moreover, both of these functions are multiplicative functions and are related by following identity:

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

For proof of this relation refer Chapter 16 of the book by Hardy-Wright[5] ◊

For some numerical results on classification of primes p into various types based on the kind of irreducible factors we get modulo p on factorizing given polyomials in Bring-Jerrard quintic form, refer §7 of [11].

[5] *An Introduction to the Theory of Numbers* (Sixth Edition), Oxford University Press, 2008.

The algorithm is very efficient since the number of operations required to factor $f(X)$ modulo p is proportional to $\log p$. As stated earlier, general reciprocity law should provide a description of the set $\mathrm{Spl}(f)$ associated with a polynomial $f(X)$. Though this algorithm is such a description, but more is wanted for it to be called a reciprocity law. The exact requirements will remain vague and undefined.

1.3 Local-Global Principle

The idea of studying something "locally" comes from the theory of functions[8]. In 1882, Richard Dedekind and Heinrich Weber[6] were the first to realize the analogy between numbers and functions. They pushed the idea that "functions are like numbers" and we can represent their analogy in following way:

$$\begin{aligned}
\text{positive integers} &\longleftrightarrow \text{polynomials} \\
\text{fractions} &\longleftrightarrow \text{quotient of polynomials} \\
\text{certain kinds of algebraic number} &\longleftrightarrow \text{elliptic functions} \\
\text{transcendental numbers} &\longleftrightarrow \text{functions like } \sin(x)
\end{aligned}$$

In particular, Dedekind and Weber showed that the techniques developed to study *algebraic numbers* could be used to study a whole class of functions, which came to be known as *algebraic functions*[7].

In 1897, Kurt Hensel[8] saw that if functions are like numbers, then numbers must be like functions. He pushed the idea that "numbers are like functions" and we can represent his analogy in following way:

$$\text{local expansions of functions} \longleftrightarrow p\text{-adic numbers}$$

If we have a prime number p, we can consider our number "locally at p" by taking their expansions in powers of p. These expansions, just like the decimal expansions, are called *p-adic expansions*. We denote the set of all possible p-adic expansions by $\mathbb{Q}_p$ which is a new realm of numbers, called *p-adic numbers*.

> For some numerical results illustrating the analogy between local expansion of functions and p-adic number, refer §2 of [8].

Just like $\mathbb{R}$ is defined as the completion of $\mathbb{Q}$ with respect to the absolute difference metric $|x-y|$, the set of of p-adic numbers $\mathbb{Q}_p$ is defined as the completion of $\mathbb{Q}$ with respect to *p-adic* metric $|x-y|_p$. We will learn more about p-adic numbers and what is

[6] Dedekind, R. and Weber, H. "Theorie Der Algebraischen Functionen Einer Veränderlichen." *Journal Für Die Reine Und Angewandte Mathematik* (Crelle's Journal) 1882, no. 92 (1882), 181–290. https://doi.org/10.1515/crll.1882.92.181

[7] Loosely speaking, these functions involve *algebraic operations* only. For example, $f(x) = \frac{\sqrt[4]{1+x^6}}{x^{5/2} - \sqrt[3]{9}x^3}$ is an algebraic function since $+, -, \times, \div, \sqrt[n]{\ }$ are the only algebraic operations. Note that x^{10} is allowed but 10^x is not allowed.

[8] Hensel, K. "Über eine neue Begründung der Theorie der algebraischen Zahlen." *Jahresbericht der Deutschen Mathematiker-Vereinigung* 6, no. 3 (1897), 83–87. http://www.digizeitschriften.de/dms/resolveppn/?PID=GDZPPN00211612X

meant by $|\cdot|_p$ in next chapter. Some general properties of p-adic numbers can be found in the article by Rozikov[13].

Note that p-adic expansions of some numbers can be different from their base-p representation. For example, in-spite of the fact that both binary and 2-adic are expansions in terms of powers of 2, they *can* have different expansions of same decimal number. This is because binary follows the absolute difference metric for notion of convergence and 2-adic follows the 2-adic metric for notion of convergence (see Theorem 13).

One may refer to the article by MacDuffee[10] to know "how to find p-adic expansions" of a given real number. Also, we can use SageMath to get p-adic expansions, just type `Qp(p,n)(m)` where `Qp(7,30)(1024)` will give 7-adic expansion of 1024 upto 30 place values i.e. from 7^0 to 7^{29}. For example, let's see various expansions of "0.2":

Type	Representation	Expansion
Decimal	0.2	$2 \cdot 10^{-1}$
Binary	$0.0011001100110011\ldots_2$	$2^{-3} + 2^{-4} + 2^{-7} + 2^{-8} + \ldots$
2-adic	$(0; 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, \ldots)_2$	$1 + 2^2 + 2^3 + 2^6 + 2^7 + 2^{10} + \ldots$
3-adic	$(0; 2, 0, 1, 2, 1, 0, 1, 2, 1, 0, 1, \ldots)_3$	$2 + 3^2 + 2 \cdot 3^3 + 3^4 + 3^6 + 2 \cdot 3^7 + 3^8 + 3^{10} + \ldots$
5-adic	$(1; 0)_5$	5^{-1}
97-adic	$(0; 39, 19, 58, 77, 38, 19, 58, 77, 38, 19, 58, \ldots)_{97}$	$39 + 19 \cdot 97 + 58 \cdot 97^2 + 77 \cdot 97^3 + 38 \cdot 97^4 + 19 \cdot 97^5 + 58 \cdot 97^6 + 77 \cdot 97^7 + 38 \cdot 97^8 + 19 \cdot 97^9 + 58 \cdot 97^{10} + \ldots$
2017-adic	$(0; 807, 403, 1210, 1613, 806, 403, 1210, 1613, 806, 403, 1210, \ldots)_{2017}$	$807 + 403 \cdot 2017 + 1210 \cdot 2017^2 + 1613 \cdot 2017^3 + 806 \cdot 2017^4 + 403 \cdot 2017^5 + 1210 \cdot 2017^6 + 1613 \cdot 2017^7 + 806 \cdot 2017^8 + 403 \cdot 2017^9 + 1210 \cdot 2017^{10} + \ldots$

In 1920, Helmut Hasse came up with an idea of possibility to answer some questions in number theory by answering them "locally"[8]. The idea was that if a Diophantine equation is solvable modulo every prime power (locally) i.e. in $\mathbb{Q}_p$, as well as in $\mathbb{R}$ then it is solvable in the integers (globally). This is known as *Hasse condition*.

Local-global principle states that the Hasse condition holds for all quadratic Diophantine equations. On the other hand, it is clear that if a polynomial $f(X) \in \mathbb{Q}[X]$ fails to have a solution over $\mathbb{Q}_p$ for some p, then it can't have a solution over $\mathbb{Q}$ (see §1.1 of [15]). We can state this principle formally as:

Theorem (Hasse-Minkowski Theorem[9]). *A quadratic form with coefficients in $\mathbb{Q}$ admits a nontrivial zero over $\mathbb{Q}$ if and only if it does so over $\mathbb{Q}_p$ for all prime numbers p and over $\mathbb{R}$.*

This theorem has become one of the guiding ideas of modern number theory[8]. For more details about the importance of this idea of "passing from local to global" one may read the article by Barry Mazur[10]. Also, this idea enables us to use reciprocity laws to study solution sets of complicated Diophantine equations, like the proof of Fermat's Last Theorem[4].

[9]Hasse, H. "Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen." *Journal Für Die Reine Und Angewandte Mathematik* (Crelle's Journal) 1923, no. 152 (1923), 205–224. https://doi.org/10.1515/crll.1923.152.205

[10]Mazur, B. "On the passage from Local to Global in Number Theory." *Bulletin of the American Mathematical Society* 29, no. 1 (1993), 14–51. https://doi.org/10.1090/s0273-0979-1993-00414-2

Chapter 2

p-adic Numbers

Major part of my exposition follows that of Prof. Chandan Singh Dalawat [2].

In my previous report[16], the concept of *number fields* was discussed. They are one of the two types of *global fields*, the other type are known as *global function fields*. Though our motive is to derive reciprocity laws (which are about global fields), our focus will be *local fields*. The reason for shifting focus to local fields is the local-global principle discussed towards the end of previous chapter. By a local field, we will understand a commutative non-discrete locally compact field[1]. Associated to each global field K is an infinite collection of local fields corresponding to the completions of K with respect to its absolute values; for the field of rational numbers $\mathbb{Q}$, these are the p-adic fields $\mathbb{Q}_p$ and the field of real numbers $\mathbb{R}$.

We begin by giving yet another formulation of quadratic reciprocity law[14]

Theorem (Quadratic reciprocity law)**.** *Let p and q be distinct odd primes, then*

$$\lambda_p(-1) = \lambda_4(p) \quad ; \quad \lambda_p(2) = \lambda_8(p) \quad ; \quad \lambda_p(q) = \lambda_q(\lambda_4(p)p)$$

where, $\lambda_p : \mathbb{F}_p^\times \to \mathbb{Z}^\times$, $\lambda_q : \mathbb{F}_q^\times \to \mathbb{Z}^\times$, $\lambda_4 : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{Z}^\times$ and $\lambda_8 : (\mathbb{Z}/8\mathbb{Z})^\times \,/\, \mathbb{Z}^\times \to \mathbb{Z}^\times$ are surjective homomorphisms of groups, called quadratic characters[2] (just like Legendre symbol).

As expected, one can prove[1] that $\lambda_4(a) = (-1)^{\frac{a-1}{2}}$ and $\lambda_8(a) = (-1)^{\frac{a^2-1}{8}}$ for any $a \in \mathbb{Z}_{(2)}$, the smallest subring of $\mathbb{Q}$ containing p^{-1} for every odd prime p.

Using this formulation we can easily extend reciprocity to cube modulo p using the ring $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ where $\omega = \frac{-1+\sqrt{-3}}{2}$ and the norm function defined as $N(a + b\omega) = a^2 - ab + b^2$[6].

Theorem (Cubic reciprocity law)**.** *Let π and θ be prime elements in $\mathbb{Z}[\omega]$ such that they have distinct norm and neither of them has norm 3, then*

$$\chi_\pi(\omega) = \omega^{\frac{N(\pi)-1}{3}}$$

$$\chi_\pi(1-\omega) = \omega^{2m} \quad \text{with} \quad \begin{cases} m = \frac{\pi+1}{3} \text{ if } \pi \text{ is a rational prime} \\ m = \frac{a+1}{3} \text{ if } \pi = a + b\omega \text{ is congruent to 2 modulo 3} \end{cases}$$

$$\chi_\pi(\theta) = \chi_\theta(\pi) \qquad \text{if } \pi \text{ and } \theta \text{ are congruent to 2 modulo 3}$$

where, $\pi = a + b\omega$ is congruent to 2 modulo 3 when $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$ and $\chi_\pi : (\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^\times \to \mathbb{Z}^\times$ is the cubic residue character.

[1] Weil, André. *Basic number theory.* (Classics in Mathematics) Berlin and Heidelberg: Springer-Verlag (1995). pp. 20

[2] If p is odd, then the order of the cyclic group $\mathbb{F}_p^\times$ is even, and there is a unique surjective morphism λ_p. If $p = 2$ then λ_4, λ_8 and $\lambda_4\lambda_8$ are the three unique quadratic characters for $(\mathbb{Z}/8\mathbb{Z})^\times$. Moreover, one can easily check that $\lambda_4(-1) = -1$ and $\lambda_8(-1) = 1$, hence $\lambda_4\lambda_8(-1) = \lambda_4(-1)\lambda_8(-1) = -1$.

p-adic numbers were the first local fields to be realized. We will first define the ring $\mathbb{Z}_p$ of p-adic integers, then will study $\mathbb{Q}_p$ as the field of fractions of $\mathbb{Z}_p$.

2.1 Ring of p-adic Integers

Let p be a prime number and n be a natural number[3]. For every $n > 0$, we define the finite ring $A_n = \mathbb{Z}/p^n\mathbb{Z}$ of p^n elements. Note that $A_1 = \mathbb{F}_p$ is the field of p elements. There is a unique morphism of rings $\varphi_n : A_{n+1} \to A_n$, called *reduction modulo* p^n and a unique morphism of groups $\eta : A_1 \to A_{n+1}$, such that $1 \mapsto p^n$. Since φ_n is surjective with $\ker(\varphi_n) = p^n A_{n+1}$ and η is injective with $\mathrm{im}(\eta) = p^n A_{n+1}$, we get following *short exact sequence*:

$$0 \longrightarrow A_1 \xrightarrow{\eta} A_{n+1} \xrightarrow{\varphi_n} A_n \longrightarrow 0$$

Definition 3 ($p-$adic integer)**.** A *p-adic integer* is a system of elements $(x_n)_{n>0}$ such that $x_n \in A_n$ and $\varphi_n(x_{n+1}) = x_n$.

A simple consequence of this definition is that, if $x_n = 0$ for some $n > 0$ then x_1 to x_{n-1} are all zero. In fact, every p-adic integer is uniquely determined by $(x_n)_{n>N}$ for any natural number $N > 0$ because $x_1 = (\varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_N)(x_{N+1})$.

Definition 4 (The set of p-adic integers)**.** The set of $p-$adic integers is denoted by $\mathbb{Z}_p$, and is defined as

$$\mathbb{Z}_p = \left\{ x \in \prod_{n>0} A_n \ : \ (\varphi_m \circ \overline{\pi}_{m+1})(x) = \overline{\pi}_m(x) \ \forall m > 0 \right\}$$

where $\overline{\pi}_m : \prod_{n>0} A_n \to A_m$ is a natural projection morphism, such that $x = (x_n)_{n>0}$ maps to x_m.

Since $\mathbb{Z}_p \subset \prod_{n>0} A_n$ and the map φ_m is surjective, we conclude that the restriction of $\overline{\pi}_m$ to $\mathbb{Z}_p$ is surjective.

Definition 5 (Algebraic operations for p-adic integers)**.** Let $x = (x_n)_{n>0}$ and $y = (y_n)_{n>0}$ be two p-adic integers, then we define:

- $x = 0$ if $x_n = 0$ for every $n > 0$
- $x = 1$ if $x_n = 1$ for every $n > 0$
- $-x = (-x_n)_{n>0}$
- $x + y = (x_n + y_n)_{n>0}$
- $xy = (x_n y_n)_{n>0}$

Theorem 1. *$\mathbb{Z}_p$ is a subring of the product ring $\prod_{n>0} A_n$, hence is a commutative ring.*

Proof. Since $0 \in \mathbb{Z}_p$, it is a non-empty subset of $\prod_{n>0} A_n$. Our definition of algebraic operations in $\mathbb{Z}_p$ enables us to use the properties of A_n. Since A_n is a (commutative) ring for every $n > 0$, if $x, y \in \mathbb{Z}_p$ then $x - y \in \mathbb{Z}_p$ and $xy \in \mathbb{Z}_p$. Therefore $\mathbb{Z}_p$ is a subring of $\prod_{n>0} A_n$. □

[3]The set of natural numbers is $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ i.e. non-negative integers. Source: ISO 80000-2:2009, "Quantities and units - Part 2: Mathematical signs and symbols to be used in the natural sciences and technology." Table 6, "Standard number sets and intervals." Item no. 2-6.1 (11.4.9).

We conclude that the restriction of $\overline{\pi}_m$ to $\mathbb{Z}_p$, $\boxed{\pi_m : \mathbb{Z}_p \to A_m}$ is a surjective morphism of rings.

Theorem 2. *$\mathbb{Z}_p$ is projective limit[4] of the inverse system $(\varphi_n : A_{n+1} \to A_n)_{n>0}$ of finite discrete rings.*

Proof. This follows from the definition of *projective limit*. An inverse system is a sequence of objects (A_n) together with a sequence of morphisms (φ_n)

$$\cdots \xrightarrow{\varphi_{n+1}} A_{n+1} \xrightarrow{\varphi_n} A_n \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_1} A_1$$

The *projective limit* $\mathbb{Z}_p = \varprojlim A_n$ is the subset of the direct product $\prod_{n>0} A_n$ consisting of those sequences $x = (x_n)_{n>0}$ for which $\varphi_n(x_{n+1}) = x_n$ for all $n > 0$. For each $n > 0$ the projection map $\pi_m : \mathbb{Z}_p \to A_m$ sends x to x_m. □

Lemma 1. *For every $m > 0$, multiplication by p^m is injective on $\mathbb{Z}_p$, and the ideal $p^m\mathbb{Z}_p$ is the $\ker(\pi_m)$.*

Proof. For the first part, it is sufficient to prove that the map $x \mapsto px$ is injective on $\mathbb{Z}_p$. Hence, we just have to prove that if for some $x \in \mathbb{Z}_p$ we have $px = 0$ then $x = 0$. Let $x = (x_n)_{n>0}$, then $px = 0$ implies that $px_n = 0$ in A_n for every $n > 0$. Since $x_1 \in \mathbb{F}_p$, $px_1 = 0$ for any value of x_1, so we consider the case $px_{n+1} = 0$ in A_{n+1} for every $n > 0$. Hence there exist $y_{n+1} \in A_{n+1}$ such that $x_{n+1} = p^n y_{n+1}$. But from the definition of p-adic integers we have $x_n = \varphi_n(x_{n+1})$ for every $n > 0$. We can use this to write $x_n = p^n\varphi_n(y_{n+1}) = 0$ in A_n for every $n > 0$, and hence $x = 0$.

For the second part, note that $p^m\mathbb{Z}_p \subset \ker(\pi_m)$ from the definition of π_m. It remains to prove that $\ker(\pi_m) \subset p^m\mathbb{Z}_p$. If $x \in \ker(\pi_m)$, then

$$\pi_m(x) = 0 = x_m = (\varphi_m \circ \varphi_{m+1} \circ \cdots \circ \varphi_{m+r-1})(x_{m+r})$$

so $x_{m+r} \in \ker(\varphi_m \circ \cdots \circ \varphi_{m+r-1}) = p^m A_{m+r}$ for every $r > 0$. But we have a short exact sequence

$$0 \longrightarrow A_r \xrightarrow{\eta_r} A_{m+r} \xrightarrow{\varphi_m \circ \cdots \circ \varphi_{m+r-1}} A_m \longrightarrow 0$$

in which the first map is the unique morphism of groups $\eta_r : A_r \to A_{m+r}$ such that $\eta_r(1) = p^m$ and $\mathrm{im}(\eta_r) = p^m A_{m+r}$. Since η_r is injective map, there is a unique $y_r \in A_r$ such that $x_{m+r} = \eta_r(y_r) = p^m y_r$. The p-adic integer $y = (y_r)_{r>0}$ is such that $\varphi_r(y_{r+1}) = y_r$ for every $r > 0$. Therefore, $x = p^m y$, and $p^m\mathbb{Z}_p = \ker(\pi_m)$. □

Theorem 3. *For every $m > 0$, the induced map $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}_p/p^m\mathbb{Z}_p$ is an isomorphism of rings.*

Proof. From Lemma 1, we have $p^m\mathbb{Z}_p \subset \mathbb{Z}_p$ and $p^m\mathbb{Z}_p = \ker(\pi_m)$. Therefore, for every $m > 0$, we have the short exact sequence

$$0 \longrightarrow p^m\mathbb{Z}_p \xrightarrow{\mathrm{id}} \mathbb{Z}_p \xrightarrow{\pi_m} A_m \longrightarrow 0$$

where id is the identity map. Apply *first isomorphism theorem*[5] to the surjective homomorphism of rings π_m to get $\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}$. □

Lemma 2. *$x \in \mathbb{Z}_p^\times$ if and only if $x \notin p\mathbb{Z}_p$*

[4] Also known as *inverse limit*.

[5] Let R be a ring. If $f : R \to S$ is a ring homomorphism, then $\ker(f)$ is an ideal of R, $f(R)$ is a subring of S and $R/\ker(f) \cong f(R)$.

Proof. ($\Rightarrow$) If $x \in \mathbb{Z}_p^\times$ then $\pi_1(x) \in \mathbb{F}_p^\times$. Since, $\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p$ from Theorem 3, we conclude that $\pi_1(x) \in \mathbb{F}_p^\times$ is equivalent to $x \notin p\mathbb{Z}_p$.

($\Leftarrow$) If $x \notin p\mathbb{Z}_p$ then $\pi_1(x) \in \mathbb{F}_p^\times$ due to the equivalence of both the statements. Since $\pi_1(x) = (\varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_{n-1})(x_n)$, it follows that for every $n > 0$, we have $x_n \notin pA_n$. Moreover, pA_n is the set of all non-unit elements of A_n, hence there exist $y_n, z_n \in A_n$ such that $x_n y_n = 1 - pz_n$, or equivalently $x_n x_n' = 1$ in A_n, with

$$x_n' = y_n \left(1 + pz_n + \ldots + p^{n-1} z_n^{n-1}\right)$$

We have $\varphi_n(x_{n+1}') = x_n'$ (because $\varphi_n(x_{n+1}')$ is also an inverse of x_n in the ring A_n), so we get a p-adic integer $x' \in \mathbb{Z}_p$ such that $xx' = 1$, and hence $x \in \mathbb{Z}_p^\times$. □

Theorem 4. *$p\mathbb{Z}_p$ is the unique maximal ideal of the ring $\mathbb{Z}_p$, i.e. $\mathbb{Z}_p$ is a local ring.*

Proof. From *Zorn's Lemma*[6] we know about the existence of at least one maximal ideal in a commutative ring with identity and that every non-unit element is contained in some maximal ideal. Therefore, a ring has unique maximal ideal if and only if the set of non-unit elements is an ideal.

In fact, we claim that the ideal $p\mathbb{Z}_p$ is the set of all non-unit elements (and hence is the unique maximal ideal). It follows from Lemma 2. □

Theorem 5. *Every $x \neq 0$ in $\mathbb{Z}_p$ can be uniquely written as $x = p^m u$, with $m \in \mathbb{N}$, $u \in \mathbb{Z}_p^\times$.*

Proof. Let $x \in \mathbb{Z}_p$. If $x \neq 0$, then as per the definition of p-adic integers, there is a smallest $m \in \mathbb{N}$ such that $\pi_{m+1}(x) \neq 0$. Then we then have $x = p^m u$ with $u \notin p\mathbb{Z}_p$. By Lemma 2, $u \in \mathbb{Z}_p^\times$. The decomposition $x = p^m u$ is unique because m is uniquely determined by x, and because $y \mapsto p^m y$ is injective, as stated in Lemma 1. □

Definition 6 (p-adic integer valuation)**.** Valuation of p-adic integer x denoted by $v_p(x)$ is defined to be $v_p(x) = m$ for $x = p^m u$ ($m \in \mathbb{N}, u \in \mathbb{Z}_p^\times$) and $v_p(0) = +\infty$.

Remark 5. From Lemma 2 it follows that $x \in \mathbb{Z}_p^\times$ if and only if $v_p(x) = 0$.

Theorem 6. *For any $x, y \in \mathbb{Z}_p$ we have:*

- $v_p(xy) = v_p(x) + v_p(y)$
- $v_p(x + y) \geq \inf(v_p(x), v_p(y))$ *with equality if* $v_p(x) \neq v_p(y)$

Proof. If at least one of x, y is zero then these statements are trivial. Let x, y be non-zero p-adic integers with $x = p^m x'$ and $y = p^n y'$ such that $x', y' \in \mathbb{Z}_p^\times$. Since $xy = p^{m+n} x'y'$, we get $v_p(xy) = m + n = v_p(x) + v_p(y)$.

Also, $x + y = p^m x' + p^n y'$. Without loss of generality, let $m \geq n$ then $x + y = p^n(p^{m-n}x' + y')$ and $v_p(x + y) \geq n = \inf(v_p(x), v_p(y))$. Moreover, for $m \neq n$, we have $p^{m-n}x' + y' \in \mathbb{Z}_p^\times$ from Lemma 2 and hence the equality holds. □

Theorem 7. *The ring $\mathbb{Z}_p$ is an integral domain and every ideal $\mathfrak{a} \neq 0$ is generated by p^n for some $n \in \mathbb{N}$, i.e. $\mathbb{Z}_p$ is a principal ideal domain.*

Proof. For $x \neq 0$ and $y \neq 0$ in $\mathbb{Z}_p$, we have $v_p(xy) = v_p(x) + v_p(y) < +\infty$ and hence $xy \neq 0$ and $\mathbb{Z}_p$ is an integral domain.

Let $\mathfrak{a} \neq 0$ be an ideal of $\mathbb{Z}_p$, and n be the smallest number in the set $v_p(\mathfrak{a})$ consisting of valuations of all elements in $\mathfrak{a}$. Our claim is that $\mathfrak{a} = p^n\mathbb{Z}_p$. Firstly, if $x \in \mathfrak{a}$ is such that $v_p(x) = n$, we have $x = p^n\alpha$ for some $\alpha \in \mathbb{Z}_p^\times$ or equivalently $p^n = x \cdot \alpha^{-1}$, so $p^n \in \mathfrak{a}$ and $p^n\mathbb{Z}_p \subset \mathfrak{a}$. Secondly, for every $y \neq 0$ in $\mathfrak{a}$, we have $v_p(y) \geq n$, and $y = p^{v_p(y)-n}\beta p^n$ for some $\beta \in \mathbb{Z}_p^\times$ by Theorem 5, so $\mathfrak{a} \subset p^n\mathbb{Z}_p$. Hence $\mathfrak{a} = p^n\mathbb{Z}_p$. □

[6] Let P be a non-empty partially ordered set, such that for every totally ordered subset L, there exists some upper bound u for L so that $u \geq x$ for every $x \in L$. Then P has a maximal element.

Definition 7 (p-adic integer absolute value)**.** Absolute value of p-adic integer x is denoted by $|x|_p$ and is defined to be $|x|_p = p^{-v_p(x)}$ for $x \neq 0$ and $|0|_p = 0$.

Theorem 8. *$d_p(x, y) = |x - y|_p$ is a metric on $\mathbb{Z}_p$.*

Proof. It is clear from definition that $d_p(x, y) \geq 0$, $d_p(x, y) = 0$ if and only if $x = y$ and $d_p(x, y) = d_p(y, x)$. From Theorem 6 it follows that for any $x, y \in \mathbb{Z}_p$ we have, $|x - y|_p \leq \sup(|x|_p, |y|_p)$ (with equality if $|x|_p \neq |y|_p$) . Hence $d_p(x, y)$ satisfies the *ultrametric inequality* $d_p(x, z) \leq \sup(d_p(x, y), d_p(y, z))$ which is stronger than (the required) triangle inequality. □

Definition 8 (Topology on $\mathbb{Z}_p$)**.** For every $m > 0$ define the subset $V_m = \pi_m^{-1}(0) = \ker(\pi_m)$ of $\mathbb{Z}_p$. There is a unique topology on $\mathbb{Z}_p$ for which $(x + V_m)_{m>0}$ is a *fundamental system of open neighbourhoods*[7] of x for every $x \in \mathbb{Z}_p$.

Each $x + V_m$ is also closed in $\mathbb{Z}_p$ because A_m is finite. This topology is compatible with the ring structure of $\mathbb{Z}_p$, and each π_m is continuous.

Theorem 9. *The space $\mathbb{Z}_p$ is compact.*

Proof. Because it is closed subset of the product $\prod_{n>0} A_n$ of finite discrete spaces. □

Theorem 10. *The topology on $\mathbb{Z}_p$ can be defined by the distance d_p, for which it is complete.*

Proof. By definition and Lemma 1, the open subsets $p^n\mathbb{Z}_p$ ($n \in \mathbb{N}$) form a fundamental system of open neighbourhoods of 0. As each of them is an open ball for d_p, namely $d_p(x, 0) < p^{-(n-1)}$, the topology on $\mathbb{Z}_p$ is the same as the one defined by d_p. That $\mathbb{Z}_p$ is complete for d_p is a consequence of its compactness (from Theorem 9), because *every compact metric space is complete*[8]. □

We can reverse the process and define $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ for the distance d_p.

Theorem 11. *The subset $\mathbb{N}$ is dense in $\mathbb{Z}_p$. More generally, if $b \in \mathbb{Z}$ is prime to p and if $a \in \mathbb{Z}$, then $a + b\mathbb{N}$ is dense in $\mathbb{Z}_p$.*

Proof. For $\mathbb{N}$ to be dense[9] in $\mathbb{Z}_p$, we need to show existence of $x' \in \mathbb{N}$ for every $x \in \mathbb{Z}_p$ and every $n > 0$, such that $x' \in x + V_n$. This follows by taking an x' whose image in A_n is x_n.

The second statement follows from this because $x \mapsto a + bx$ is an *isometry*[10] of $\mathbb{Z}_p$ whenever $\gcd(b, p) = 1$, as $|b|_p = 1$. □

Theorem 12. *The set $\mathbb{Z}_p$ has the cardinality of the continuum.*

Proof. As seen in section 1.3, for every $n > 0$, base-p expansion in $\mathbb{N}$ gives a natural bijection from $[0, p[^n = \{x \in \mathbb{Z} \ : \ 0 \leq x < p\}$ to $[0, p^n[= \{x \in \mathbb{Z} \ : \ 0 \leq x < p^n\}$, namely

$$(b_i)_{i \in [0,n[} \mapsto \sum_{i \in [0,n[} b_i p^i$$

and hence a natural bijection $[0, p[^n \to A_n$.

[7] A collection $\mathcal{V}$ of neighbourhoods of x is called a fundamental system of neighbourhoods of x if for any neighbourhood M of x there exists a finite sequence $V_1, V_2, \ldots, V_n$ of neighbourhoods in $\mathcal{V}$ such that $x \in V_1 \cap V_2 \ldots \cap V_n \subset M$.

[8] This is easy to prove because for a metric space, compactness is equivalent to sequential compactness.

[9] A subset A of a topological space X is dense in X if for any point $x \in X$, any neighbourhood of x contains at least one point from A.

[10] Given two metric spaces, X and Y, a map $f : X \to Y$ is said to be an isometry if for any $a, b \in X$ one has $d_X(a, b) = d_Y(f(a), f(b))$ where d_X and d_Y are metric functions for X and Y respectively.

If $x_{n+1} \in A_{n+1}$ corresponds to $(b_i)_{i\in[0,n]}$, then $\varphi_n(x_{n+1})$ corresponds to $(b_i)_{i\in[0,n[}$. The set $\mathbb{Z}_p$ is in natural bijection with the product $[0,p[^{\mathbb{N}}$. A p-adic integer $x \in \mathbb{Z}_p$ and a sequence $(b_i)_{i\in\mathbb{N}} \in [0,p[^{\mathbb{N}}$ correspond to each other if and only if

$$\pi_n(x) \equiv \sum_{i\in[0,n[} b_i p^i \pmod{p^n}$$

(in A_n) for every $n > 0$. It follows that the set $\mathbb{Z}_p$ has the cardinality of the continuum. □

Theorem 13. *To every p-adic integer $x \in \mathbb{Z}_p$, if we associate a sequence $(b_i)_{i\in\mathbb{N}}$ of elements $b_i \in [0,p[$ characterised by the fact that for every $n \in \mathbb{N}$,*

$$\sum_{i\in[0,n]} b_i p^i \equiv \pi_{n+1}(x) \pmod{p^{n+1}}$$

Then for every $x \in \mathbb{Z}_p$, the associated series $\sum_{i\in\mathbb{N}} b_i p^i$ converges in $\mathbb{Z}_p$ to x.

Proof. For every $n \in \mathbb{N}$, let $s_n = \sum_{i\in[0,n]} b_i p^i$ be the partial sums, and fix an integer $m > 0$. We have to show that *almost all*[11] s_n are in $x + p^m\mathbb{Z}_p$. This is clearly the case as soon as $n > m$, for $s_n - x \in p^{n+1}\mathbb{Z}_p$, by the defining property of the sequence $(b_i)_{i\in\mathbb{N}}$. □

So a p-adic integer x can be considered as a formal expression $x = \sum_{i\in\mathbb{N}} b_i p^i$, with $b_i \in [0,p[$. Addition and multiplication can be defined by interpreting the partial sums as elements of $\mathbb{N}$ and taking base-p expansions of the sum or product. For $x \neq 0$, the valuation $v_p(x)$ is the smallest index i such that $b_i \neq 0$. The greater the valuation of x, the closer x is to 0 in the p-adic sense of $d_p(0,x)$. For example, the sequence $1, p, p^2, \ldots$ converges to 0 in $\mathbb{Z}_p$.

2.2 Hensel's Lemma

Now let's prove the central theorem of p-adic analysis. Then will use this theorem to build theory needed to handle reciprocity laws.

Definition 9 (Formal derivative)**.** Given a ring R (not necessarily commutative) and $A = R[X]$. The formal derivative is an operation on elements of A, where if $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ then its formal derivative is $f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$.

Lemma 3. *If the ring R of scalars is commutative with $f(X) \in R[X]$ then*

$$f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$$

for some $g(X,Y) \in R[X,Y]$.

Proof. We just need to simplify using binomial expansion.

$$\begin{aligned}
f(X+Y) &= a_n(X+Y)^n + a_{n-1}(X+Y)^{n-1} + \ldots + a_1(X+Y) + a_0 \\
&= a_n\left(X^n + nX^{n-1}Y + \ldots + nXY^{n-1} + Y^n\right) + \ldots + a_1(X+Y) + a_0 \\
&= (a_nX^n + \ldots + a_0) + \left(na_nX^{n-1} + \ldots + a_1\right)Y + \left(a_n\binom{n}{2}X^{n-2} + \ldots + a_2\right)Y^2 \\
&= f(X) + f'(X)Y + g(X,Y)Y^2
\end{aligned}$$

for some $g(X,Y) \in R[X,Y]$. □

[11] "Almost all" is sometimes used synonymously with "all except finitely many" or "all except a countable set". We are using this terminology from *measure theory*. For example, if measure assigns to a subregion of the rectangle the fraction of the geometrical area it occupies. Then the rectangle's boundary has measure 0 and its interior has measure 1. We conclude that *almost every* point of the rectangle is an interior point, yet the interior has a nonempty complement.

Definition 10 (Simple root)**.** Let R be a ring and $f(X) \in R[X]$ then x is said to be a simple root of $f(X)$ in some ring A if $f(x) = 0$ in A but $f'(x) \neq 0$ in A.

Definition 11 (Hensel's lifting)**.** Given $f(X) \in \mathbb{Z}_p[X]$ with a simple root x in $A_m = \mathbb{Z}_p/p^m\mathbb{Z}_p$, then y is said to be Hensel's lifting of x in $A_{m+1} = \mathbb{Z}_p/p^{m+1}\mathbb{Z}_p$ if

- $y = x + p^m z$ for some $z \in \mathbb{Z}_p$
- $y \equiv x \pmod{p^m}$
- $f(y) \equiv 0 \pmod{p^{m+1}}$
- $f'(y) \not\equiv 0 \pmod{p}$

Lemma 4. *If $f(X) \in \mathbb{Z}_p[X]$ has a simple root in $A_1 = \mathbb{Z}_p/p\mathbb{Z}_p$, then it can be uniquely lifted to a root of $f(X)$ in $A_2 = \mathbb{Z}_p/p^2\mathbb{Z}_p$.*

Proof. Let $x_0 \in \mathbb{Z}_p$ be the simple root of $f(X)$ in A_1, hence $f(x_0) \equiv 0 \pmod{p}$ but $f'(x_0) \not\equiv 0 \pmod{p}$. We will improve x_0 to $x_1 = x_0 + pz_1$ (with $z_1 \in \mathbb{Z}_p$, so that $x_1 \equiv x_0 \pmod{p}$) such that $f(x_1) \equiv 0 \pmod{p^2}$. To compute $f(x_0 + pz_1)$ we use Lemma 3, so $f(x_1) \equiv f(x_0) + f'(x_0)z_1 p \pmod{p^2}$. As $f(x_0) = y_0 p$ for some $y_0 \in \mathbb{Z}_p$,

$$f(x_0 + z_1 p) \equiv 0 \pmod{p^2} \quad \Leftrightarrow \quad y_0 + f'(x_0)z_1 \equiv 0 \pmod{p}$$

Since $f'(x_0) \not\equiv 0 \pmod{p}$, we can take $z_1 = -\frac{y_0}{f'(x_0)} = -\frac{f(x_0)}{pf'(x_0)}$, and then

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}, \quad f(x_1) \equiv 0 \pmod{p^2}, \quad x_1 \equiv x_0 \pmod{p}$$

Moreover, $f'(x_1) \equiv f'(x_0) \not\equiv 0 \pmod{p}$. □

We will use *Hensel's lifting*, an analogue of the *Newton's method*, for solving polynomial equations. Suppose we want to find a root $\xi \in \mathbb{Z}_p$ of some polynomial $f(X) \in \mathbb{Z}_p[X]$. This amounts to finding, for every $n > 0$, a root $\xi_n \in A_n$ of $f(X)$ such that $\xi_{n+1} \equiv \xi_n \pmod{p^n}$ where $\xi = (\xi_n)_{n>0}$. So a first necessary condition for ξ to exist is that there should exist an $x_0 \in \mathbb{Z}_p$ such that $f(x_0) \equiv 0 \pmod{p}$.

Theorem 14 (Hensel's Lemma)**.** *Let $f(X) \in \mathbb{Z}_p[X]$ and $x \in \mathbb{Z}_p$ be such that $f'(x) \neq 0$, and put $\delta = v_p(f'(x))$. Suppose that we have $f(x) \equiv 0 \pmod{p^m}$ for some $m > 2\delta$. Then there exists a unique $\xi \in \mathbb{Z}_p$ such that $f(\xi) = 0$ and $\xi \equiv x \pmod{p^{m-\delta}}$. Moreover, $v_p(f'(\xi)) = \delta$.*

Proof. We will prove this theorem in three steps.

Step 1. Generalize the concept of "lift" by deriving analogous properties for $y = x - \frac{f(x)}{f'(x)}$.

Since $\delta = v_p(f'(x))$, we can write $f'(x) = p^\delta u$ for some $u \in \mathbb{Z}_p^\times$. Without loss of generality, we can write $f(x) = p^m a$ for some $a \in \mathbb{Z}_p$. We just need check all the conditions for this value of y to be the "generalized lift".

Note that, $x - y = \frac{f(x)}{f'(x)} = p^{m-\delta}\frac{a}{u} \in p^{m-\delta}\mathbb{Z}_p$, therefore $\boxed{y \equiv x \pmod{p^{m-\delta}}}$. (This implies that $y \equiv x \pmod{p^m}$ if x is a simple root, since then $\delta = 0$).

Using Lemma 3 and evaluating the value of $f(y)$, we can write

$$f(y) = f(x + y - x) = f(x) + f'(x)(y - x) + t(y - x)^2$$

for some $t \in \mathbb{Z}_p$. Now using our claimed value of y in right hand side, we get:

$$\begin{aligned} f(y) &= f(x) - f'(x)\frac{f(x)}{f'(x)} + t\left(\frac{f(x)}{f'(x)}\right)^2 \\ &= t\left(\frac{f(x)}{f'(x)}\right)^2 \end{aligned}$$

Therefore, $f(y) \in p^{2m-2\delta}\mathbb{Z}_p$ and because $m > 2\delta$ we get $\boxed{f(y) \equiv 0 \pmod{p^{m+1}}}$.

Again using Lemma 3 and evaluating the value of $f'(y)$, we can write

$$f'(y) = f'(x + y - x) = f'(x) + s(y - x)$$

for some $s \in \mathbb{Z}_p$. Now using Theorem 6 we can write

$$\begin{aligned} v_p(f'(y)) &= v_p(f'(x) + s(y - x)) \\ &\geq \inf\left(v_p(f'(x)), v_p(s(y - x))\right) \\ &= \inf\left(\delta, v_p(s) + v_p(y - x)\right) \end{aligned}$$

Since $m - \delta > \delta$, we have $v_p(y - x) + v_p(s) > \delta$. Therefore, $\boxed{v_p(f'(y)) = \delta}$ (and $f'(y) \not\equiv 0 \pmod{p}$ if x is a simple root since then $\delta = 0$).

Step 2. Show the existence of ξ.

We put $x = x_0$ and $y = x_1$, then we can apply previous step to x_1 to obtain $x_2 = x_1 - \frac{f(x_1)}{f'(x_1)}$ such that $x_2 \equiv x_1 \pmod{p^{m+1-\delta}}$, $f(x_2) \equiv 0 \pmod{p^{m+2}}$ and $v_p(f'(x_2)) = \delta$. We can iterate previous step to get a sequence of p-adic integers $x_0, x_1, \ldots, x_i, \ldots$ such that

- $x_{i+1} = x_i + \frac{f(x_i)}{f'(x_i)}$
- $x_{i+1} \equiv x_i \pmod{p^{m+i-\delta}}$
- $f(x_i) \equiv 0 \pmod{p^{m+i}}$
- $v_p(f'(x_i)) = \delta$

for all $i \in \mathbb{N}$. If we put $\xi = (\xi_n)_{n>0}$ with $\xi_{m+i} = \pi_{m+i}(x_i)$ for $i \in \mathbb{N}$ then $\boxed{\xi \equiv x \pmod{p^{m-\delta}}}$. We claim that this ξ is the solution of $f(X)$. Hence we have to prove that $f(\xi) = 0$. Note that since $f(X)$ is a polynomial, we can use Definition 5 to get

$$f(\xi) = (f(\xi_1), f(\xi_2), \ldots, f(\xi_m), \ldots)$$

Hence for given m we conclude that:

$$f(\xi_{m+i}) = f(\pi_{m+i}(x_i)) = \pi_{m+i}(f(x_i)) = 0$$

in A_{m+i} for all $i \in \mathbb{N}$. Since, $f(\xi) \in \mathbb{Z}_p$ we have $\varphi_{m-1}(f(\xi_m)) = f(\xi_{m-1}) = 0$ hence it follows that $f(\xi_n) = 0$ for all $n < m$. Therefore, $\boxed{f(\xi) = 0}$.

Step 3. Show uniqueness of ξ.

On the contrary assume that there exist $\xi' \in \mathbb{Z}_p$ such that $f(\xi') = 0$ with $\xi' \equiv x \pmod{p^{\delta+1}}$. Note that is a weaker condition than required in the theorem since $m - \delta \geq \delta + 1$. Using Lemma 3 and evaluating the polynomial, we get

$$f(\xi') = f(\xi + \xi' - \xi) = f(\xi) + f'(\xi)(\xi' - \xi) + b(\xi' - \xi)^2$$

for some $b \in \mathbb{Z}_p$. But $f(\xi) = f(\xi') = 0$, hence

$$0 = 0 + f'(\xi)(\xi' - \xi) + +b(\xi' - \xi)^2$$

Since $\xi' \neq \xi$ we get:

$$f'(\xi) + (\xi' - \xi)b = 0$$

This implies that $v_p(f'(\xi)+(\xi'-\xi)b) = \infty$. But since $v_p(f'(\xi)) = \delta$ and $v_p((\xi'-\xi)b) > \delta$ (as seen in Step 1 above), we have $v_p(f'(\xi) + (\xi' - \xi)b) = \delta$ by Theorem 6. We get a contradiction since $f'(x) \neq 0$ implies that $\delta < \infty$, completing the proof.

□

Definition 12 (Quadratic character of p-adic unit integer)**.** Given $u \in \mathbb{Z}_p^\times$, we define $\lambda_p(u) = \lambda_p(\pi_1(u))$ for any odd prime p, otherwise (for $p = 2$) $\lambda_4(u) = \lambda_4(\pi_2(u))$ and $\lambda_8(u) = \lambda_8(\pi_3(u))$, where π_m is the projection $\mathbb{Z}_p^\times \to (\mathbb{Z}/p^m\mathbb{Z})^\times$.

Lemma 5. *For primes $p \neq 2$, a unit $u \in \mathbb{Z}_p^\times$ is a square if and only if $\lambda_p(u) = +1$.*

Proof. ($\Rightarrow$) For every $u = x^2 \in \mathbb{Z}_p^\times$, $\lambda_p(u) = \lambda_p(x^2) = +1$ (since $\lambda_p(x)$ can only be $+1$ or -1).

($\Leftarrow$) Suppose that $\lambda_p(u) = +1$. Then there exists an $x \in \mathbb{Z}_p$ such that $f(x) \equiv 0 \pmod p$, where $f(X) = X^2 - u$. Since $u \in \mathbb{Z}_p^\times$, $x \not\equiv 0 \pmod p$ therefore $f'(x) = 2x \not\equiv 0 \pmod p$. Since $f'(x) \neq 0$, we can apply Theorem 14 with $\delta = v_p(2x) = v_p(2) + v_p(x) = 0 + 0 = 0$ and $m = 1$, to conclude that there is a unique $\xi \in \mathbb{Z}_p$ such that $f(\xi) = 0$, $\xi \equiv x \pmod p$, and $v_p(f'(\xi)) = 0$ (which just means that $\xi \in \mathbb{Z}_p^\times$). In other words, $u = \xi^2$ for some unique $\xi \in \mathbb{Z}_p^\times$. □

Theorem 15. *For odd primes p, the $\mathbb{F}_2$-space[12] $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}$ consists of $\{\bar{1}, \bar{u}\}$, where u is any unit such that $\lambda_p(u) = -1$.*

Proof. From Lemma 5 we conclude that $x \in \mathbb{Z}_p^{\times 2}$ if and only if $\lambda_p(x) = +1$, since $\mathbb{Z}_p^{\times 2}$ is the subgroup of $\mathbb{Z}_p^\times$ containing all squares. The existence of a unit $u \in \mathbb{Z}_p^\times$ with $\lambda(u) = -1$ follows from the fact that the projection $\pi_1 : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ is surjective. □

Lemma 6. *For any $u \in \mathbb{Z}_2^\times$ we have $\lambda_4(u) = +1$ and $\lambda_8(u) = +1$ if and only if $u \equiv 1 \pmod 8$.*

Proof. By Theorem 3 we have $(\mathbb{Z}_2/8\mathbb{Z}_2)^\times = (\mathbb{Z}/8\mathbb{Z})^\times$ which is a 2-dimensional vector space over $\mathbb{F}_2$. Also, $\mathbb{Z}^\times$ is 1-dimensional vector space over $\mathbb{F}_2$. Then, as per definitions of λ_4 and λ_8 we know that λ_4 and λ_8 are the basis elements of $\mathrm{Hom}_{\mathbb{F}_2}((\mathbb{Z}/8\mathbb{Z})^\times, \mathbb{Z}^\times)$ (see pt. 11 on pp. 4 of [1]). For any $x \in (\mathbb{Z}/8\mathbb{Z})^\times$, following theorem from linear algebra

> Let $\mathbb{F}$ be a field, V and W be a finite dimensional vector space over $\mathbb{F}$ with $\dim_{\mathbb{F}}(V) = n$ and $\dim_{\mathbb{F}}(W) = 1$. Then $V^* = \mathrm{Hom}_{\mathbb{F}}(V, W)$ is also a finite dimensional vector space over $\mathbb{F}$ with $\dim_{\mathbb{F}}(V^*) = n$ which behaves just like the dual space of V. Therefore, we can choose $f_1, f_2 \ldots, f_n$ as basis of v^* over $\mathbb{F}$ such that for any $x \in V$ we have $f_1(x), \ldots, f_n(x) \in W$. This implies that, $x = 0$ if and only if $f_1(x) = f_2(x) = \ldots = f_n(x) = 0$, where 0 is the identity element of V and W.

□

[12] Note that here vectors spaces are multiplicatively written, hence the linear combination look like $x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n}$ instead of conventional $c_1x_1 + c_2x_2 + \ldots + c_nx_n$ for x_i belong to vector space and c_i belong to the field.

implies that, $x = 1$ if and only if $\lambda_4(x) = \lambda_8(x) = 1$ (since here vector spaces are multiplicatively written). In other words, for any $x \in \mathbb{Z}_2^\times$ we have $u \equiv 1 \pmod 8$ if and only if $\lambda_4(u) = +1$ and $\lambda_8(u) = +1$.

Lemma 7. *Given $u \in \mathbb{Z}_2^\times$ is a square if and only if $\lambda_4(u) = +1$ and $\lambda_8(u) = +1$.*

Proof. ($\Rightarrow$) For every $u = x^2 \in \mathbb{Z}_2^\times$, $\lambda_4(u) = \lambda_4(x^2) = +1$ and $\lambda_8(u) = \lambda_8(x^2) = +1$.

($\Leftarrow$) Suppose that $\lambda_4(u) = +1 = \lambda_8(u)$. Then there exist $x \in \mathbb{Z}_2$ such that[13] $f(x) \equiv 0 \pmod 8$, where $f(X) = X^2 - u$. Also, by Lemma 6, given condition implies that $u \equiv 1 \pmod 8$. Therefore, $x \equiv 1 \pmod 8$ leading to $f(1) \equiv 0 \pmod 8$ and $f'(1) = 2 \neq 0$. Now, we can apply Theorem 14 with $\delta = v_2(2) = 1$ and $m = 3$, to conclude that there is a unique $\xi \in \mathbb{Z}_2$ such that $f(\xi) = 0$, $\xi \equiv 1 \pmod 4$, and $v_2(f'(\xi)) = 1 = v_2(2\xi)$ (which just means that $\xi \in \mathbb{Z}_2^\times$). In other words, $u = \xi^2$ for some unique $\xi \in \mathbb{Z}_2^\times$. □

Theorem 16. *The $\mathbb{F}_2$-space $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2}$ has a basis consisting of $\bar{5}, -\bar{1}$. The values of λ_4, λ_8 on this basis are given by the table*[14]

	$\bar{5}$	$-\bar{1}$
λ_4	1	-1
λ_8	-1	1

Proof. From Lemma 7 we conclude that $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} = (\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{5}, -\bar{1}, -\bar{5}\}$ is isomorphic to Klein four-group and hence is generated by $\bar{5}$ and $-\bar{1}$. The values of λ_4, λ_8 on this basis are computed using the definition of λ_4 and λ_8. □

Definition 13 (Section map)**.** Given a map $f : A \to B$, then $g : B \to A$ is called the section map if $(g \circ f)(x) = \mathrm{id}(x)$.

Theorem 17. *Let $R \subset \mathbb{Z}_p$ be the set of roots of $X^p - X$. The reduction map $\pi_1 : \mathbb{Z}_p \to \mathbb{F}_p$ gives a bijection $R \to \mathbb{F}_p$. Moreover, if $x, y \in R$, then $xy \in R$ and if $\omega : \mathbb{F}_p \to R$ denotes the reciprocal bijection, then $\omega(ab) = \omega(a)\omega(b)$.*

Proof. Put $f(X) = X^p - X$ and since $\mathbb{F}_p$ is a finite field, every $a \in \mathbb{F}_p$ is a simple root of $f(X) \pmod p$. So by Theorem 14 for $\delta = 0, m = 1$, there is a unique root $\omega(a) \in R$ of $f(X)$ in $\mathbb{Z}_p$ such that $\omega(a) \equiv a \pmod p$. In other words, $\pi_1(\omega(a)) = a$. Since R is the set of roots in an integral domain $\mathbb{Z}_p$ of a polynomial of degree p, it can have at most p elements. Therefore the map $\omega : \mathbb{F}_p \to R$ is bijective, and π_1 induces the reciprocal bijection.

If $x, y \in R$, then $x^p = x$ and $y^p = y$, therefore $(xy)^p = xy$, and hence $xy \in R$. Finally, the multiplicativity $\omega(ab) = \omega(a)\omega(b)$ for $a, b \in \mathbb{F}_p$ follows from the uniqueness of the $\omega(ab) \in R$ such that $\pi_1(\omega(ab)) = ab$ (by Theorem 14) and the fact that for the element $\omega(a)\omega(b) \in R$ we have $\pi_1(\omega(a)\omega(b)) = ab$. □

Here $\omega : \mathbb{F}_p \to \mathbb{Z}_p$ is canonical *section* of the projection $\pi_1 : \mathbb{Z}_p \to \mathbb{F}_p$. Though ω cannot be a morphism (of groups or rings), but it has the desirable property of being *multiplicative*. The subset R is called *the set of multiplicative representatives of $\mathbb{F}_p$ in $\mathbb{Z}_p$*.

2.3 Group of Unit p-adic Integers

Definition 14 (Subgroup of units of $\mathbb{Z}_p$)**.** For every $n > 0$, let $U_n = 1 + p^n\mathbb{Z}_p$ be the group of units in $\mathbb{Z}_p$ which are $\equiv 1 \pmod{p^n}$.

[13] We are not using $f(x) \equiv 0 \pmod 4$ because we need $m > 2\delta$ and in this case $\delta = 1$.

[14] We follow the same convention as in *Cayley table* i.e. the factor that labels the row comes first, and the factor that labels column is second.

The U_n form a decreasing sequence of *open subgroups*[15]

$$\cdots \subset U_n \subset U_{n-1} \subset \cdots \subset U_2 \subset U_1$$

of $\boxed{U = \mathbb{Z}_p^\times}$, hence U can be identified with the projective limit of the system $(\varphi_n : U/U_{n+1} \to U/U_n)_{n>0}$ (as in Theorem 2). Moreover, each U_m can be identified with the projective limit of the system $(\varphi_{m+r} : U_m/U_{m+r+1} \to U_m/U_{m+r})_{r>0}$.

Let $R^\times$ be the set of roots of $X^{p-1} - 1$ in $\mathbb{Z}_p$. We sometimes identify $\mathbb{F}_p^\times$ with $R^\times \subset \mathbb{Z}_p^\times$. The morphism of groups, $\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ is a *section* (as in Theorem 17) of the short exact sequence

$$1 \longrightarrow U_1 \xrightarrow{\text{id}} \mathbb{Z}_p^\times \xrightarrow{\pi_1} \mathbb{F}_p^\times \longrightarrow 1, \qquad \mathbb{F}_p^\times \xrightarrow{\omega} \mathbb{Z}_p^\times$$

where id is the identity map (compare with the short exact sequence in Theorem 3 for $m = 1$).

Theorem 18. *For every prime p, the group $\mathbb{Z}_p^\times$ is the internal direct product*[16] *of $R^\times$ and U_1.*

Proof. We need to check both the conditions of internal direct product. Both subgroups are normal because $\mathbb{Z}_p^\times$ is abelian. Also if $x \in R^\times \cap U_1$ then $x^{p-1} = 1$ and $x = 1 + py$ for some $y \in \mathbb{Z}_p$. Therefore $y = 0$ and $R^\times \cap U_1 = \{1\}$. Moreover, every $x \in \mathbb{Z}_p^\times$ can be written as $x = ab$, with $a = \omega(\pi_1(x))$ in $R^\times$ and $b = xa^{-1}$ in U_1. □

Lemma 8. *The group U_n/U_{n+1} is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Proof. For every $x \in \mathbb{Z}_p$ and $n > 0$ we have the identity

$$(1 + p^n x)(1 + p^n y) \equiv 1 + p^n(x + y) \pmod{p^{n+1}}$$

Hence $x \mapsto (x-1)/p^n \pmod p$ is a surjective morphism of groups $U_n \to \mathbb{F}_p$, and its kernel is U_{n+1}. Therefore, the map $(1 + p^n x) \mapsto \pi_1(x)$ defines upon passage to the quotient an isomorphism of groups $U_n/U_{n+1} \to \mathbb{Z}/p\mathbb{Z}$ by first isomorphism theorem[17]. □

Lemma 9. *If $x \in U_n$ but $x \notin U_{n+1}$, then $x^p \in U_{n+1}$ but $x^p \notin U_{n+2}$ for $n > 0$ if p is an odd prime and $n > 1$ if $p = 2$. In other words, $(\ )^p$ induces an isomorphism $U_n/U_{n+1} \to U_{n+1}/U_{n+2}$ of groups (of order p).*

Proof. Write $x = 1 + p^n a$, so that $a \not\equiv 0 \pmod p$, by hypothesis. The binomial theorem gives

$$x^p = (1 + p^n)^p = 1 + \binom{p}{1}(p^n a) + \ldots + \binom{p}{p}(p^n a)^p = 1 + p^{n+1}a + \ldots + p^{np}a^p$$

where the suppressed terms $\binom{p}{r}(p^n a)^r$ $(1 < r < p)$ are all divisible by p^{2n+1} and hence also by p^{n+2}. At the same time, we have $np > n + 1$ (because $n > 1$ if $p = 2$), so we get $x^p \equiv 1 + p^{n+1}a \pmod{p^{n+2}}$, which implies that $x^p \in U_{n+1}$ but $x^p \notin U_{n+2}$. The induced morphism $U_n/U_{n+1} \to U_{n+1}/U_{n+2}$ is an isomorphism because it is not trivial and the two groups are of order p. Thus we have following commutative diagram of groups:

[15] We are talking about topological groups. A collection G of elements is called a topological group provided the collection satisfies the following axioms: (1) G is group; (2) G is a topological space; (3) the group operations $g_1 g_2$ and g^{-1} are continuous functions in the topology of the space.

[16] The two conditions to be satisfied are: (1) Both the given subgroups are normal subgroups; (2) Their intersection has only identity element and every element of the group can be written as product of two elements taking one element from each subgroup.

[17] Let G be a group. If $f : G \to H$ is a group homomorphism, then $\ker(f)$ is normal subgroup of G, $f(G)$ is a subgroup of H and $G/\ker(f) \cong f(G)$.

$$\begin{array}{ccc} U_n & \xrightarrow{(\ )^p} & U_{n+1} \\ \downarrow & & \downarrow \\ U_n/U_{n+1} & \xrightarrow{\sim} & U_{n+1}/U_{n+2} \end{array}$$

Therefore the map $(\ )^p$ takes U_n to U_{n+1}, the composite map $U_n \to U_{n+1}/U_{n+2}$ is surjective, its kernel in U_{n+1} for every $n > 0$ if $p \neq 2$ and $n > 1$ if $p = 2$. □

Theorem 19. *The group U_n/U_{n+r} is cyclic of order p^r for every $r > 0$ with $n > 0$ if $p \neq 2$ and $n > 1$ if $p = 2$.*

Proof. Choose an x (for example $x = 1 + p^n$) such that $x \in U_n$ but $x \notin U_{n+1}$. By repeated application of Lemma 9, we see that $x^{p^i} \in U_{n+i}$ but $x^{p^i} \notin U_{n+i+1}$ for every $i > 0$.

$$\begin{array}{ccc} U_n & \xrightarrow{(\ )^{p^i}} & U_{n+i} \\ \downarrow & & \downarrow \\ U_n/U_{n+i} & \xrightarrow{\sim} & U_{n+i}/U_{n+i+1} \end{array}$$

Let's denote the image of x in U_n/U_{n+r} by x_r. Then put $i = r - 1$ to get $x^{p^{r-1}} \notin U_{n+r}$ which implies that $(x_r)^{p^{r-1}} \neq 1$ and $i = r$ to get $x^{p^r} \in U_{n+r}$ which implies that $(x_r)^{p^r} = 1$. Therefore x_r has order p^r.

Moreover, the group U_n/U_{n+r} has a *filtration*[18]

$$U_{n+r}/U_{n+r} \subset U_{n+r-1}/U_{n+r} \subset \cdots \subset U_{n+1}/U_{n+r} \subset U_n/U_{n+r}$$

whose successive quotients $(U_{n+i}/U_{n+r})/(U_{n+i+1}/U_{n+r}) = U_{n+i}/U_{n+i+1}$ have order p as in Lemma 8. Since subgroup indices are multiplicative[19] and if N is a normal subgroup of G, then the index of N in G is also equal to the order of the quotient group[20] G/N, we conclude U_n/U_{n+r} that has order p^r.

Therefore U_n/U_{n+r} is cyclic and x_r is a generator. □

Corollary 1. *Let $x \in U_n$ (with $n > 0$ if $p \neq 2$ and $n > 1$ if $p = 2$) and denote by x_r the image of x in U_n/U_{n+r}, for every $r > 0$. There is a unique morphism of groups $f_{x,r} : \mathbb{Z}/p^r\mathbb{Z} \to U_n/U_{n+r}$ such that $f_{x,r}(1) = x_r$. If $x \notin U_{n+1}$, then $f_{x,r}$ is an isomorphism.*

Theorem 20. *U_n/U_{n+r} is a $(\mathbb{Z}/p^r\mathbb{Z})$-module (multiplicatively written). As such, it is free of rank 1.*

Proof. Fix $\bar{x} \in U_n/U_{n+r}$. For every $a \in \mathbb{Z}$, the power $\bar{x}^a$ depends only on the class $\bar{a} \in \mathbb{Z}/p^r\mathbb{Z}$, and we put $\bar{x}^{\bar{a}} = \bar{x}^a$. The law $(\bar{a}, \bar{x}) \mapsto \bar{x}^{\bar{a}}$ makes U_n/U_{n+r} into a multiplicatively written $(\mathbb{Z}/p^r\mathbb{Z})$-module. From Theorem 19 we know that U_n/U_{n+r} is cyclic, hence it is free of rank 1. □

Theorem 21. *Let $x \in U_n$ with $n > 0$ if $p \neq 2$ and $n > 1$ if $p = 2$. There is a unique morphism[21] of groups $f_x : \mathbb{Z}_p \to U_n$ such that if $a = (a_r)_{r>0}$ (with $a_r \in \mathbb{Z}/p^r\mathbb{Z}$) and*

[18] It is an indexed set S_i of subobjects of a given algebraic structure S with the index i running over some index set I that is totally ordered subject to condition that $i \leq j$ in I then $S_i \subseteq S_j$.

[19] If you have $K < H < G$, then $[G : K] = [G : H][H : K]$

[20] Since this is defined in terms of a group structure on the set of cosets of N in G.

[21] Here we consider the additive group structure of $\mathbb{Z}_p$. The point is that the additive structure of $\mathbb{Z}_p$ is relatively easy to understand. By showing the isomorphism, it makes the multiplicative structure of $\mathbb{Z}_p$ relatively easy to understand as well.

$x = (x_r)_{r>0}$ *(with* $x_r \in U_n/U_{n+r}$*), then* $f_x(a) = (x_r^{a_r})_{r>0}$*. If* $x \notin U_{n+1}$*, then* f_x *is an isomorphism.*

Proof. Recall that U_n is the projective limit of the inverse system $(\varphi_{n+r} : U_n/U_{n+r+1} \to U_n/U_{n+r})_{r>0}$ and we have following commutative diagram in which $f_{x,r}(1) = x_r$ for every $r > 0$ as in Corollary 1

$$\begin{array}{ccc} \mathbb{Z}/p^{r+1}\mathbb{Z} & \xrightarrow{f_{x,r+1}} & U_n/U_{n+r+1} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^r\mathbb{Z} & \xrightarrow{f_{x,r}} & U_n/U_{n+r} \end{array}$$

Hence there is a unique morphism of groups $f_x : \mathbb{Z}_p \to U_n$ inducing the $f_{x,r}$. We have $f_x(1) = x$. If $x \notin U_{n+1}$, then f_x is an isomorphism because every $f_{x,r}$ is an isomorphism. □

Remark 6. One can define p-adic versions of $\log$ and $\exp$ functions to compute these maps; these maps are just as useful in doing p-adic calculations as their real analogues are. This group isomorphism is comparable to the fact that the multiplicative group of positive real numbers is isomorphic to the additive group of all real numbers. ◊

Corollary 2. *The group* U_1 *is isomorphic to* $\mathbb{Z}_p$ *for* $p \neq 2$ *and the group* U_2 *is isomorphic to* $\mathbb{Z}_2$ *for* $p = 2$*.*

Proof. Isomorphism follows from previous theorem. If p is odd then $x = 1 + p \in U_1$ but $x \notin U_2$ so $\mathbb{Z}_p \cong U_1$ as groups. If $p = 2$ then $x = 1 + 2^2 \in U_2$ but $x \notin U_3$ so $\mathbb{Z}_2 \cong U_2$. □

Theorem 22. $\mathbb{Z}_2^\times = U_1$ *is the internal direct product of* $\mathbb{Z}^\times$ *and* U_2*.*

Proof. Since $x \in \mathbb{Z}_2^\times$ iff $x \notin 2\mathbb{Z}_p$ (by Lemma 2) and $\mathbb{Z}_2/2\mathbb{Z}_p \cong \mathbb{Z}/2\mathbb{Z}$ (by Theorem 3), we have $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2 = U_1$. As in Theorem 18, we just need to check the conditions of internal direct product, moreover every $x \in \mathbb{Z}_2^\times$ can be uniquely written as $x = su$ $(s \in \mathbb{Z}^\times, u \in U_2)$. □

Corollary 3. *For* $p = 2$*, the restriction of* $\lambda_8 : \mathbb{Z}_2^\times \to \mathbb{Z}^\times$ *to* U_2 *induces the unique isomorphism* $U_2/U_3 \to \mathbb{Z}^\times$*. Conversely,* λ_8 *can be recovered from this isomorphism via the projection* $\mathbb{Z}_2^\times/\mathbb{Z}^\times \to U_2$ *(which can be written* $a \mapsto \lambda_4(a)a$*).*

Theorem 23. U_n *is a* $\mathbb{Z}_p$*-module (multiplicatively written). As such, it is free of rank* 1*.*

Proof. For $a \in \mathbb{Z}_p$ and $x \in U_n$, the law $x^a = f_x(a) = (x_r^{a_r})_{r>0}$ makes U_n into a multiplicatively written $\mathbb{Z}_p$-module. As seen in Theorem 20, it is a free $\mathbb{Z}_p$-module of rank 1. □

This means that $U_n \cong \mathbb{Z}_p$ as groups along with some extra data about the $\mathbb{Z}_p$-action on the group, as seen in Corollary 2.

Corollary 4. *For every* $a \in \mathbb{Z}_p^\times$ *and for every* $n > 0$*, the map* $(\ )^a : U_n \to U_n$ *is an isomorphism.*

Proof. This follows from the facts that each U_n is a $\mathbb{Z}_p$-module (by Theorem 23) and a is invertible in $\mathbb{Z}_p$ (by Lemma 2). □

2.4 Group of Units in A_n

Definition 15 (Group of units in A_n)**.** $G_{p^n} = \mathbb{Z}_p^\times / U_n = (\mathbb{Z}/p^n\mathbb{Z})^\times$ is multiplicative group of units in $A_n = \mathbb{Z}/p^n\mathbb{Z}$.

Lemma 10. *Let $p \neq 2$ be a prime and let $n > 0$. The projection $\varpi_1 : G_{p^n} \to \mathbb{F}_p^\times$ has a canonical section, and G_{p^n} is canonically isomorphic[22] to $\mathbb{F}_p^\times \times (U_1/U_n)$. The group U_1/U_n is cyclic of order p^{n-1} and it is generated by $1+p$.*

Proof. Note that $G_{p^n} = \mathbb{Z}_p^\times / U_n$. We know the structure of $\mathbb{Z}_p^\times$ from Lemma 2, hence can show existence of canonical section as in Theorem 17. The isomorphism follows from Theorem 18. Also, we've seen that U_1/U_n is cyclic of order p^{n-1} and generated by $1+p$ in Theorem 19 and Corollary 2. □

Lemma 11. *Let $n > 1$. The projection $\varpi_1 : G_{2^n} \to G_{2^2}$ has a canonical section, and G_{2^n} is canonically isomorphic to $\mathbb{Z}^\times \times (U_2/U_n)$. The group U_2/U_n is cyclic of order 2^{n-2} and it is generated by $1+2^2$.*

Proof. Note that $G_{2^n} = \mathbb{Z}_2^\times / U_n$. We know the structure of $\mathbb{Z}_2^\times$ from Lemma 2, hence can show existence of canonical section as in Theorem 17. The isomorphism follows from Theorem 22. Also, we've seen that U_2/U_n is cyclic of order p^{n-2} and generated by $1+2^2$ in Theorem 19 and Corollary 2. □

Theorem 24. *G_{p^n} $(n > 0)$ is cyclic for every prime $p \neq 2$, and G_{2^n} $(n > 1)$ is cyclic if and only if $n = 2$.*

Proof. It follows from the previous two lemmas. □

2.5 Field of p-adic Numbers

Definition 16 (Field of p-adic numbers)**.** Let p be a prime number. We define $\mathbb{Q}_p$ to be the field of fractions of $\mathbb{Z}_p$.

Theorem 25. *Every $x \neq 0$ in $\mathbb{Q}_p$ can be uniquely written as $x = p^m u$, with $m \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$.*

Proof. Since every $x \neq 0$ in $\mathbb{Z}_p$ can be uniquely written as $x = p^m u$ where $m \in \mathbb{N}$ and $u \in \mathbb{Z}_p^\times$ (by Theorem 5), we have $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, and every $x \neq 0$ in $\mathbb{Q}_p$ can be uniquely written as $x = p^m u$ where $m \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$) □

Definition 17 (p-adic valuation)**.** Valuation of p-adic number x is the value of homomorphism $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ denoted by $v_p(x)$ and is defined to be $v_p(x) = m$ for $x = p^m u$ $(m \in \mathbb{Z}, u \in \mathbb{Z}_p^\times)$ and $v_p(0) = +\infty$.

This new definition of v_p extends our earlier definition, hence Theorem 6 holds for $x, y \in \mathbb{Q}_p$.

Definition 18 (p-adic integer absolute value)**.** Absolute value of p-adic number x is the value of homomorphism[23] $|\ |_p : \mathbb{Q}_p^\times \to \mathbb{R}_+^\times$ denoted by $|x|_p$ and is defined to be $|x|_p = p^{-v_p(x)}$ for $x \neq 0$ and $|0|_p = 0$.

[22] Internal direct product is equivalent to external direct product. If G is an internal direct product of subgroups N_1 and N_2, then G is isomorphic to external direct product $N_1 \times N_2$ via the isomrphism map $(a, b) \mapsto ab$ from $N_1 \times N_2$ to G. Conversely, given an external direct product G of groups A and B, then we can find subgroups in $G = A \times B$ isomorphic to A and B respectively, whose internal direct product is $A \times B$.

[23] Here, $\mathbb{R}_+^\times$ denotes the multiplicative group of positive real numbers.

This new definition of $|x|_p$ extends our earlier definition, hence Theorem 8 holds for $\mathbb{Q}_p$ and $|a+b|_p \leq \sup(|a|_p + |b|_p)$ for $a, b \in \mathbb{Q}_p$.

Remark 7. For every $m \in \mathbb{Z}$, we have the sub-$\mathbb{Z}_p$-module of $\mathbb{Q}_p$ generated by p^m, and the inclusion $p^{m+1}\mathbb{Z}_p \subset p^m\mathbb{Z}_p$; the union of this increasing sequence (when $m \to -\infty$) is $\mathbb{Q}_p$.

Theorem 26. *The field $\mathbb{Q}_p$ is locally compact, complete for d_p, and the subring $\mathbb{Z}[\frac{1}{p}]$ is dense.*

Proof. From Theorem 9 we know that $\mathbb{Z}_p$ is compact ; as it is defined as a subspace of $\mathbb{Q}_p$ by $d_p(0,x) < p$, it is an open neighbourhood of 0. Therefore $\mathbb{Q}_p$ is locally compact and, like any locally compact commutative group, complete.

We have seen in Theorem 13 that every $x \in \mathbb{Z}_p$ can be uniquely written as $\sum_{n\in\mathbb{N}} b_n p^n$, with $b_i \in [0, p[$. It follows that every $x \in \mathbb{Q}_p$ can be uniquely written as $\sum_{n\geq v_p(x)} b_n p^n$, making x the limit of the sequence $(s_m)_m$ of partial sums of the series representing x. But each s_m is in $\mathbb{Z}[\frac{1}{p}]$, so $\mathbb{Z}[\frac{1}{p}]$ is dense in $\mathbb{Q}_p$. □

Definition 19 (Uniformiser)**.** An element $\ell \in \mathbb{Q}_p$ is called a uniformiser if $v_p(\ell) = 1$.

The simplest example is $\ell = p$.

Definition 20 (Splitting)**.** A short exact sequence

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

is said to split if there exists either a homomorphism $\bar{f} : B \to A$ with $\bar{f} \circ f = \mathrm{id}$ or a homomorphism $\bar{g} : C \to B$ with $g \circ \bar{g} = \mathrm{id}$ (these maps are examples of sections).

Theorem 27. *If p is an odd prime then $\mathbb{Q}_p^\times = \mathbb{Z} \times \mathbb{F}_p^\times \times \mathbb{Z}_p$, otherwise $\mathbb{Q}_2^\times = \mathbb{Z} \times \mathbb{Z}^\times \times \mathbb{Z}_2$*

Proof. The choice of a uniformiser ℓ leads to the splitting $\beta : 1 \mapsto \ell$ of the short exact sequence

$$1 \longrightarrow \mathbb{Z}_p^\times \xrightarrow{\mathrm{id}} \mathbb{Q}_p^\times \underset{\beta}{\overset{v_p}{\rightleftarrows}} \mathbb{Z} \longrightarrow 0$$

and thus to an isomorphism $(m, u) \mapsto \ell^m u$ of groups $\mathbb{Z} \times \mathbb{Z}_p^\times \to \mathbb{Q}_p^\times$ by the following theorem

> A short exact sequence
>
> $$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$
>
> splits with a $\bar{g} : C \to B$ if and only if there is a homomorphism $\Theta : C \to \mathrm{Aut}(A)$ such that $B \cong A \rtimes_\Theta C$. However, when B is abelian, C acts trivially on A, so $A \rtimes_\Theta C = A \times C$. For proof see: "Splitting of Short Exact Sequences for Groups" by Keith Conrad[a].
>
> [a] http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/splittinggp.pdf

Along with ℓ, if we also choose a generator α of the free rank-1 $\mathbb{Z}_p$-module U_1 when $p \neq 2$ then $\mathbb{Q}_p^\times = \mathbb{Z} \times \mathbb{F}_p^\times \times \mathbb{Z}_p$ (by Theorem 18, Theorem 23 and Theorem 24).

Along with ℓ, if we also choose a generator α of the free rank-1 $\mathbb{Z}_2$-module U_2 when $p = 2$ then $\mathbb{Q}_2^\times = \mathbb{Z} \times \mathbb{Z}^\times \times \mathbb{Z}_2$ (by Theorem 22, Theorem 23 and Theorem 24).

For example, we could take $\alpha = 1 + p$ when $p \neq 2$ and $\alpha = 1 + 2^2$ when $p = 2$. □

Theorem 28. *If $p \neq 2$, the group $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ consists of $\{\bar{1}; \bar{u}; \bar{p}, \bar{u}\bar{p}\}$, where $u \in \mathbb{Z}_p^\times$ is any unit such that $\lambda_p(u) = -1$.*

Proof. This follows immediately from the isomorphism in Theorem 27 and the fact that $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2} = \{1, \bar{u}\}$ (from Theorem 15). □

Theorem 29. *We have* $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} = \{\bar{1}; \bar{5}; -\bar{1}, -\bar{5}; \bar{2}, \overline{10}, -\bar{2}, -\overline{10}\}$.

Proof. This follows immediately from the isomorphism in Theorem 27 and the fact that $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} = \{\bar{1}; \bar{5}; -\bar{1}, -\bar{5}\}$ (from Theorem 16). □

Definition 21 (Unramified Quadratic character)**.** For every p, the morphism $\mu_p(x) = (-1)^{v_p(x)}$ is a quadratic character of $x \in \mathbb{Q}_p^\times$.

Remark 8. Choosing a uniformiser ℓ, we get a retraction[24] $x \mapsto x\ell^{-v_p(x)}$ of the inclusion $\mathbb{Z}_p^\times \to \mathbb{Q}_p^\times$, allowing us to view λ_p (quadratic characters of $\mathbb{Z}_p^\times$) as *ramified* quadratic characters of $\mathbb{Q}_p^\times$. We extend the domain to $\mathbb{Q}_p^\times$ by $\lambda_p(x) = \lambda_p(t)$ if $x = p^m t$ with $m \in \mathbb{Z}, t \in \mathbb{Z}_p^\times$. Similarly for λ_4 and λ_8. ◊

We choose the uniformiser $\ell = p$ to fix ideas.

Corollary 5. *For $p \neq 2$, the quadratic characters μ_p, λ_p constitute a basis of the $\mathbb{F}_2$-space $\mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{Z}^\times)$. Their values on the basis $\bar{u}, \bar{p}$ of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ are given by the table*

	$\bar{u}$	$\bar{p}$
μ_p	1	-1
λ_p	-1	1

Corollary 6. *The quadratic characters $\mu_2, \lambda_4, \lambda_8$ constitute a basis[25] of the $\mathbb{F}_2$-space $\mathrm{Hom}(\mathbb{Q}_2^\times, \mathbb{Z}^\times)$. Their values on the basis $\bar{5}, -\bar{1}, \bar{2}$ of $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ are given by the table*

	$\bar{5}$	$-\bar{1}$	$\bar{2}$
μ_2	1	1	-1
λ_4	1	-1	1
λ_8	-1	1	1

2.6 Quadratic Hilbertian Symbol

Definition 22 (Quadratic hilbertian symbol)**.** The quadratic hilbertian symbol $(\ ,\ )_p : \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \to \mathbb{Z}^\times$ for $a, b \in \mathbb{Q}_p^\times$ is defined as[26]

$$(a,b)_p = \begin{cases} \lambda_p(\gamma_{a,b}) & \text{if } p \neq 2 \\ (-1)^{\alpha_2\beta_0 + \alpha_1\beta_1 + \alpha_0\beta_2} & \text{if } p = 2 \end{cases}$$

where $\gamma_{a,b} = (-1)^{v_p(a)v_p(b)} a^{v_p(b)} b^{-v_p(a)} \in \mathbb{Z}_p^\times$ and for $\bar{a}, \bar{b} \in \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$,

$$\bar{a} = 5^{\alpha_2} \cdot (-1)^{\alpha_1} \cdot 2^{\alpha_0}, \quad \bar{b} = 5^{\beta_2} \cdot (-1)^{\beta_1} \cdot 2^{\beta_0}, \quad (\alpha_i, \beta_j \in \mathbb{Z}/2\mathbb{Z})$$

Theorem 30. *For $a, b \in \mathbb{Q}_p^\times$ we have*

- ⋆ $(a,b)_p = (b,a)_p$
- ⋆ $(a,bc)_p = (a,b)_p(a,c)_p$
- ⋆ $(a,-a)_p = 1$

[24] A continuous map of a space into a subspace leaving each point of the subspace fixed.
[25] Also have a look at proof of Lemma 6.
[26] If we try to express it in terms of μ_p then it will become messy since $(\mu_p(a))^{v_p(b)} = \left((-1)^{v_p(a)}\right)^{v_p(b)}$.

Proof. For $p = 2$ these statements directly follow from the symmetry in the formula of $(a, b)_2$.

For $p \neq 2$, the first statement follows from the fact that interchanging a, b replaces $\gamma_{a,b}$ by $\gamma_{a,b}^{-1}$, but $\lambda_p(\gamma_{a,b}^{-1}) = \lambda_p(\gamma_{a,b})$ since $\lambda_p : \mathbb{Z}_p^\times \to \mathbb{Z}^\times$ is a unique surjectve morphism, therefore $\lambda_p(1) = \lambda_p(uu^{-1}) = \lambda_p(u)\lambda_p(u^{-1}) = 1$ and $\lambda_p(u) = \lambda_p(u^{-1}) = \pm 1$ for all $u \in \mathbb{Z}_p^\times$. The second statement follows from the fact that $v_p(bc) = v_p(b) + v_p(c)$ and laws of exponent. The third statement follows from the fact that $\gamma_{a,-a} = 1$ and $\lambda_p(1) = 1$. □

Remark 9. It follows from these facts that $(a, b)_p$ depends only on the classes of a, b modulo $\mathbb{Q}_p^{\times 2}$ in the sense that $(a, b)_p = (ac^2, b)_p$ for every $c \in \mathbb{Q}_p^\times$ and $(a, b)_p = (a, bd^2)_p$ for every $d \in \mathbb{Q}_p^\times$. ◊

Theorem 31. *Let p be an odd prime and $a, b \in \mathbb{Z}_p^\times$. Then*

- $(a, b)_p = 1$
- $(a, pb)_p = \lambda_p(a)$

Proof. Both statements follow directly from the definition, since $v_p(a) = v_p(b) = 0$, $v_p(p) = 1$. Therefore $\gamma_{a,b} = 1$ and $\gamma_{a,pb} = a^{v_p(pb)} = a^{v_p(b)+v_p(p)} = a$. □

Theorem 32. *Let $a, b \in \mathbb{Z}_2^\times$. Then we have*

- $(a, b)_2 = (-1)^{\varepsilon_4(a)\varepsilon_4(b)}$
- $(a, 2)_2 = (-1)^{\varepsilon_8(a)} = \lambda_8(a)$

where $\varepsilon_4(c), \varepsilon_8(c) \in \mathbb{F}_2$ are defined for $c \in \mathbb{Z}_2^\times$ by $\lambda_4(c) = (-1)^{\varepsilon_4(c)}$, $\lambda_8(c) = (-1)^{\varepsilon_8(c)}$ with λ_4, λ_8 are the quadratic characters of $\mathbb{Z}_2^\times$ coming from the identifications $(\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{Z}^\times$ and $(\mathbb{Z}/8\mathbb{Z})^\times/\mathbb{Z}^\times \to \mathbb{Z}^\times$.

Proof. By Lemma 2 we know that $\bar{a} = 5^{\alpha_2}(-1)^{\alpha_1}$ and $\bar{b} = 5^{\beta_2}(-1)^{\beta_1}$, therefore $(a, b)_2 = (-1)^{\alpha_1\beta_1}$. By Theorem 16 we get $\alpha_1 = \varepsilon_4(a)$, $\beta_1 = \varepsilon_4(b)$, therefore $(a, b)_2 = (-1)^{\varepsilon_4(a)\varepsilon_4(b)}$.

Since $\bar{2} = 2^1$, we get $(a, 2)_2 = (-1)^{\alpha_2}$. By Theorem 16 we get $\alpha_2 = \varepsilon_8(a)$, therefore $(a, 2)_2 = (-1)^{\varepsilon_8(a)}$. □

Theorem 33. *For a given prime number p we have*

$$(p, p)_p = \begin{cases} \lambda_p(-1) & \text{if } p \neq 2 \\ 1 & \text{if } p = 2 \end{cases}$$

Proof. Using Theorem 30 we can write $(p, p)_p = (-p, p)_p(-1, p)_p = (-1, p)_p$, which equals $\lambda_p(-1)$ if $p \neq 2$ (by Theorem 31), and $\lambda_8(-1) = 1$ if $p = 2$ (by Theorem 32). □

Corollary 7. *For every p, the pairing $(\ ,\ )_p$ is* invertible *in the sense that its Cayley table, for $p \neq 2$ and $p = 2$ respectively (with $\lambda_4(p) = \lambda_p(-1)$ by quadratic reciprocity law)*

$(\ ,\ )_p$	u	p
u	1	-1
p	-1	$\lambda_4(p)$

$(\ ,\ )_2$	5	-1	2
5	1	1	-1
-1	1	-1	1
2	-1	1	1

when expressed as matrices (with entries in $\mathbb{Z}^\times$) with respect to the given basis of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ is invertible (when viewed with entries in the field $\mathbb{F}_2$). Indeed, in $\mathbb{F}_2$,

$$\begin{vmatrix} 0 & 1 \\ 1 & \varepsilon_4(p) \end{vmatrix} = 1 \qquad \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} = 1$$

Lemma 12. *Let $a, b \in \mathbb{Q}_p^\times$. If $a + b = 1$, then $(a, b)_p = 1$.*

Proof. We will divide the proof in two cases and their sub-cases.

Case 1. $p \neq 2$

(a) $v_p(a) > 0$
Since $b = 1 - a$ and $a = p^m u$ has $m > 0$ for some $u \in \mathbb{Z}$, we conclude that $b \equiv 1 \pmod{p}$. Hence $b \in U_1 \subset \mathbb{Z}_p^\times$ and $b = t^2$ for some $t \in U_1$ because from Corollary 4 we know that $(\ )^2 : U_1 \to U_1$ is bijective. So, $(a, b)_p = (a, t^2)_p = 1$ (as in Remark 9).

(b) $v_p(a) = 0$ and $v_p(b) = 0$
Then, $(a, b)_p = 1$ by Theorem 31.

(c) $v_p(a) < 0$
Let $a = p^{-n}u$ from some $n > 0$ and $u \in \mathbb{Z}_p^\times$. We need to consider two sub-cases

i. n is even
We can multiple a and b by p^n without disturbing the value of $(a, b)_p$ to get $(a, b)_p = (u, p^n - u)_p$. Now, $p^n - u = b \equiv -u \pmod{p}$ hence it's a unit and we can use Theorem 31 to conclude that $(a, b)_p = 1$.

ii. n is odd
We can multiply a and b by p^{n+1} without disturbing the value of $(a, b)_p$ to get

$$\begin{aligned}
(a, b)_p &= (pu, p^{n+1} - pu)_p \\
&= (p, p(p^n - u))_p (u, p(p^n - u))_p \quad \text{(Theorem 30)} \\
&= (p, p)_p (p, p^n - u)_p (u, p)_p (u, p^n - u)_p \quad \text{(Theorem 30)} \\
&= \lambda_p(-1) \cdot \lambda_p(p^n - u) \cdot \lambda_p(u) \cdot 1 \quad \text{(Theorem 31 \& Theorem 33)} \\
&= \lambda_p(-1) \cdot \lambda_p(-u) \cdot \lambda_p(u) \quad (\because\ p^n - u \equiv -u \pmod{p^n}) \\
&= \lambda_p(u^2) \quad (\because\ \lambda_p \text{ is a morphism}) \\
&= 1
\end{aligned}$$

Case 2. $p = 2$

Note that $a, b \in \mathbb{Z}_2^\times$ is impossible because the equation $1 + 1 = 1$ does not hold in $\mathbb{F}_2$.

(a) $v_2(a) > 2$
Since $b = 1 - a$ and $a = 2^m u$ has $m > 2$ for some $u \in \mathbb{Z}_2^\times$, we conclude that $b \equiv 1 \pmod{2^3}$. Hence $b \in U_3 = U_2^2$ because from Lemma 9 we know that $(\ )^2 : U_2 \to U_3$ is a surjective map. So, $(a, b)_2 = (a, t^2)_2 = 1$ (as in Remark 9).

(b) $v_2(a) = 2$
Let $a = 2^2 u$ for some $u \in \mathbb{Z}_2^\times$, then $b = 1 - 2^2 u \equiv 1 \pmod{2^2}$ and hence $b \in U_2 \subset \mathbb{Z}_2^\times$. So we can write

$$\begin{aligned}
(a, b)_2 &= (2^2 u, 1 - 2^2 u)_2 \\
&= (u, 1 - 2^2 u)_2 \quad \text{(as in Remark 9)} \\
&= (-1)^{\varepsilon_4(u)\varepsilon_4(1-2^2u)} \quad \text{(Theorem 32)} \\
&= (-1)^{\varepsilon_4(u)\varepsilon_4(1)} \quad (\because\ 1 - 2^2 u \equiv 1 \pmod{2^2}) \\
&= 1 \quad (\because\ \lambda_4(1) = 1 \Rightarrow \varepsilon_4(1) = 0)
\end{aligned}$$

(c) $v_2(a) = 1$

Let $a = 2u$ for some $u \in \mathbb{Z}_2^\times$, then $b = 1 - 2u \equiv 1 \pmod 2$ and hence $b \in U_1 \subset \mathbb{Z}_2^\times$. So we can write

$$\begin{aligned}(a,b)_2 &= (2u, 1-2u)_2 \\ &= (2, 1-2u)_2 (u, 1-2u)_2 \quad \text{(Theorem 30)} \\ &= \lambda_8(1-2u) \cdot (-1)^{\varepsilon_4(u)\varepsilon_4(1-2u)} \quad \text{(Theorem 32)}\end{aligned}$$

We can't simplify it further, rather we will work modulo 8 (in $G_8 = (\mathbb{Z}/8\mathbb{Z})^\times$) and list the various possibilities using Theorem 16

$u =$	1	5	-5	-1	$\in G_8$
$\lambda_8(1-2u) =$	1	1	-1	-1	$\in \mathbb{Z}^\times$
$\varepsilon_4(u) =$	0	0	1	1	$\in \mathbb{F}_2$
$\varepsilon_4(1-2u) =$	1	1	1	1	$\in \mathbb{F}_2$

Therefore, $(a,b)_2 = 1$ in this case since this is so for each possibility.

(d) $v_2(a) < 0$ Let $a = 2^{-n}u$ from some $n > 0$ and $u \in \mathbb{Z}_p^\times$. We need to consider two sub-cases

i. n is even

We can multiple a and b by 2^n without disturbing the value of $(a,b)_p$, then $b = 1 - 2^n u \equiv 1 \pmod 2^n$ and hence $b \in U_n \subset \mathbb{Z}_2^\times$. So we can write

$$\begin{aligned}(a,b)_2 &= (u, 2^n - u)_2 \\ &= (-1)^{\varepsilon_4(u)\varepsilon_4(2^n-u)} \quad \text{(Theorem 32)} \\ &= (-1)^{\varepsilon_4(u)\varepsilon_4(-u)} \quad (\because\ 2^n - u \equiv -u \pmod{2^2}) \\ &= (-1)^{\varepsilon_4(u)(1+\varepsilon_4(u)} \quad (\because\ \lambda_4(-u) = (-1)^{\varepsilon_4(-u)} = -\lambda_4(u)) \\ &= 1 \quad (\because\ t(1+t) \equiv 0 \pmod 2\ \forall t \in \mathbb{Z})\end{aligned}$$

ii. n is odd

We can multiply a and b by 2^{n+1} without disturbing the value of $(a,b)_2$ to get

$$\begin{aligned}(a,b)_2 &= (2u, 2^{n+1} - 2u)_2 \\ &= (2, 2(2^n - u))_2 (u, 2(2^n - u))_2 \quad \text{(Theorem 30)} \\ &= (2,2)_2 (2, 2^n - u)_2 (u, 2)_2 (u, 2^n - u)_2 \quad \text{(Theorem 30)} \\ &= \lambda_8(2^n - u)\lambda_8(u)(-1)^{\varepsilon_4(u)\varepsilon_4(2^n-u)} \quad \text{(Theorem 32, Theorem 33)}\end{aligned}$$

We can't simplify it further, rather we will work modulo 8 (in G_8) and list the various possibilities using Theorem 16. Since $n \equiv 1 \pmod 2$, we have to consider two cases for n i.e. $n = 1$ and $n \geq 3$ since we are working with π_2 and π_3 (as in Definition 12).

	$u =$	1	5	-5	-1	$\in G_8$
$\lambda_8(2^n - u)$	$\lambda_8(2-u) =$	1	-1	1	-1	$\in \mathbb{Z}^\times$
	$\lambda_8(-u) =$	1	-1	-1	1	$\in \mathbb{Z}^\times$
	$\lambda_8(u) =$	1	-1	-1	1	$\in \mathbb{Z}^\times$
	$\varepsilon_4(u) =$	0	0	1	1	$\in \mathbb{F}_2$
$\lambda_8(2^n - u)$	$\varepsilon_4(2-u) =$	0	0	1	1	$\in \mathbb{F}_2$
	$\varepsilon_4(-u) =$	1	1	0	0	$\in \mathbb{F}_2$

Therefore, $(a,b)_2 = 1$ in this case since this is so for each possibility.

This completes the verification. □

Theorem 34. *Let $a, b \in \mathbb{Q}_p^\times$. There exist $x, y \in \mathbb{Q}_p$ such that $ax^2 + by^2 = 1$ if and only if $(a, b)_p = 1$.*

Proof. ($\Rightarrow$) Suppose that there do exist $x, y \in \mathbb{Q}_p$ such that $ax^2 + by^2 = 1$.

Case 1. $x = 0$ (resp. $y = 0$)

Then b (resp. a) is in $\mathbb{Q}_p^{\times 2}$, and hence $(a, b)_p = 1$ (as in Remark 9).

Case 2. $xy \neq 0$

Then $(a, b)_p = (ax^2, by^2)_p = 1$ by Lemma 12.

($\Leftarrow$) Suppose that $(a, b)_p = 1$. Since the value $(a, b)_p$ as well as the existence of x, y depend only on the classes of a and b modulo $\mathbb{Q}_p^{\times 2}$, we need only consider the following cases (Theorem 28 & Theorem 29)

Case 1. $v_p(a) = v_p(b) = 0$

Thus, we have $a, b \in \mathbb{Z}_p^\times$.

(a) $p \neq 2$

In this case $(a, b)_p = 1$ is trivially true (Theorem 31). Consider $\bar{a} = \pi_1(a) \in \mathbb{F}_p$ and $\bar{b} = \pi_1(b) \in \mathbb{F}_p$ and the following two subsets

$$S = \left\{\bar{a}\alpha^2 \ : \ \alpha \in \mathbb{F}_p\right\}, \quad T = \left\{1 - \bar{b}\beta^2 \ : \ \beta \in \mathbb{F}_p\right\}$$

Note that both of these sets have equal number of elements i.e. zero and all quadratic resides[27] modulo p. Thus

$$|S| = |T| = 1 + \frac{p-1}{2} = \frac{p+1}{2}$$

Since both S and T are subsets of $\mathbb{F}_p$ but $|S \cup T| = p < p + 1 = |S| + |T|$. We conclude that, $|S \cap T| > 0$ and there exist α, β such that $\bar{a}\alpha^2 = 1 - \bar{b}\beta^2$. Hence there exist[28] $x, y \in \mathbb{Z}_p$ such that $ax^2 + by^2 \equiv 1 \pmod{p}$. Now following two instances are possible

i. $x \not\equiv 0 \pmod{p}$
Then the unit $(1 - by^2)a^{-1}$ is a square modulo p, and hence the square of some $t \in \mathbb{Z}_p^\times$. We then have $at^2 + by^2 = 1$.

ii. $x \equiv 0 \pmod{p}$
Then for the same reason $b = t^2$ for some $t \in \mathbb{Z}_p^\times$, and we have $a \cdot 0^2 + b \cdot (t^{-1})^2 = 1$ in $\mathbb{Q}_p$.

(b) $p = 2$

As $(a, b)_2 = (-1)^{\varepsilon_4(a)\varepsilon_4(b)} = 1$, we may suppose (up to interchanging a and b) that $a \equiv 1 \pmod 4$ (Theorem 16); equivalently

i. $a \equiv 1 \pmod 8$
There is a $t \in \mathbb{Z}_2^\times$ such that $a = t^2$ (Lemma 6 & Lemma 7) and hence $a(t^{-1})^2 + b.0^2 = 1$ in $\mathbb{Q}_2$.

ii. $a \equiv 5 \pmod 8$
Since $b \in \mathbb{Z}_2^\times$, $b \not\equiv 0 \pmod 2$; equivalently $b \equiv 1 \pmod 2$. So $4b \equiv 4 \pmod 8$, and we have $a + 4b \equiv 1 \pmod 8$. Hence there is a $t \in \mathbb{Z}_2^\times$ such that $t^2 = a + 4b$ (Lemma 6 & Lemma 7). We then have $a \cdot (t^{-1})^2 + b \cdot (2t^{-1})^2 = 1$, in $\mathbb{Q}_2$.

[27] For proof of the fact that number of quadratic residues modulo p is $\frac{p-1}{2}$, refer to Theorem 1.5.1 (Euler's Criterion) on 9 of [15].

[28] This is NOT equivalent to saying that there exist $x, y \in \mathbb{Q}_p$ such that $ax^2 + by^2 = 1$.

Case 2. $v_p(a) = 0$ and $v_p(b) = 1$

Thus, we have $a \in \mathbb{Z}_p^\times$ and $b \in p\mathbb{Z}_p^\times$.

(a) $p \neq 2$

Let $b = pu$ for some $u \in \mathbb{Z}_p^\times$. Then the hypothesis $(a,b)_p = \lambda_p(a) = 1$ (Theorem 31) implies that there is a $t \in \mathbb{Z}_p^\times$ such that $a = t^2$ (Lemma 5). Hence $a(t^{-1})^2 + b.0^2 = 1$.

(b) $p = 2$

Let $b = 2u$ for some $u \in \mathbb{Z}_p^\times$. Then the hypothesis $(a,b)_2 = (a,2)_2(a,u)_2 = \lambda_8(a)(-1)^{\varepsilon_4(a)\varepsilon_4(u)} = 1$ (Theorem 30 & Theorem 32) is equivalent to

i. $\lambda_8(a) = 1$ with $\varepsilon_4(a) = 0$ or $\varepsilon_4(u) = 0$

This is equivalent to saying $a \equiv -1 \pmod 8$ with $a \equiv 1 \pmod 4$ or $u \equiv 1 \pmod 4$ (Theorem 16). Therefore, $a \equiv -1 \pmod 8$ and $u \equiv 1 \pmod 4$ (and $\varepsilon_4(a) = 1$). This can be re-written as $a \equiv -1 \pmod 8$ and $b \equiv 2 \pmod 8$, which implies that $a + b \equiv 1 \pmod 8$ and hence $a + b = t^2$ for some $t \in \mathbb{Z}_2^\times$ (Lemma 6 & Lemma 7). So, we have $a(t^{-1})^2 + b(t^{-1})^2 = 1$ in $\mathbb{Q}_2$

ii. $\lambda_8(a) = -1$ with $\varepsilon_4(a) = \varepsilon_4(u) = 1$

This is equivalent to saying $a \equiv 5 \pmod 8$ with $a \equiv -1 \pmod 4$ and $u \equiv -1 \pmod 4$ (Theorem 16). Therefore, this situation in not possible.

Case 3. $v_p(a) = v_p(b) = 1$

This case can be reduced to the previous case upon replacing a by $-ab^{-1}$ because $v_p(-ab^{-1}) = v_p(-1) + v_p(a) - v_p(b) = 0 + 1 - 1 = 0$. Firstly, by Theorem 30 and Remark 9 we get

$$(-ab^{-1}, b)_p = (a,b)_p(-b^{-1}, b)_p = (a,b)_p(-b, b)_p = (a,b)_p$$

Secondly, the existence of $x, y \in \mathbb{Q}_p$ such that $-ab^{-1}x^2 + by^2 = 1$ is equivalent to the existence of $(x,y,z) \neq (0,0,0)$ in $\mathbb{Q}_p^3$ such that $-ab^{-1}x^2 + by^2 = z^2$ by the following general lemma

> Let k any field of characteristic $\neq 2$, and let $a, b \in k^\times$. If there is a pair $(x,y) \in k^2$ such that $ax^2 + by^2 = 1$, then certainly there is a triple $(x,y,s) \neq (0,0,0)$ such that $ax^2 + by^2 = s^2$.
> Conversely, if there is such a triple, then there is a desired pair. This is clear if $s \neq 0$. If $s = 0$ (in which case $x \neq 0$ and $y \neq 0$), we have $-a = \frac{b}{t^2}$ with $t = \frac{y}{x}$ and $a\left(\frac{a+1}{2a}\right)^2 + b\left(\frac{a-1}{2at}\right)^2 = 1$, so a suitable pair exists.

Multiplying throughout by b and rearranging, the latter becomes $ax^2 + bz^2 = (by)^2$, which can be seen as before to be equivalent to the existence of $x, y \in \mathbb{Q}_p$ such that $ax^2 + by^2 = 1$.

□

Definition 23 (Norm homomorphism)**.** Let $b \in \mathbb{Q}_p^\times$, and put $K_b = \mathbb{Q}_p(\sqrt{b})$, so that the degree $[K_b : \mathbb{Q}_p]$ equals 1 or 2 according as $b \in \mathbb{Q}_p^{\times 2}$ or $b \notin \mathbb{Q}_p^{\times 2}$. We have the norm homomorphism $N_b : K_b^\times \to \mathbb{Q}_p^\times$ defined as

$$N_b\left(x + y\sqrt{b}\right) = \begin{cases} x + y\sqrt{b} & \text{if } [K_b : \mathbb{Q}_p] = 1 \Leftrightarrow b \in \mathbb{Q}_p^{\times 2} \\ x^2 - by^2 & \text{if } [K_b : \mathbb{Q}_p] = 2 \Leftrightarrow b \notin \mathbb{Q}_p^{\times 2} \end{cases}$$

for any $x, y \in \mathbb{Q}_p$.

Theorem 35. *Let $a, b \in \mathbb{Q}_p^\times$. We have $(a,b)_p = 1$ if and only if $a \in N_b(K_b^\times)$.*

Proof. We will prove the equivalence in both the possible cases separately.

Case 1. $b \in \mathbb{Q}_p^{\times 2}$

Then $N_b(K_b^\times) = \mathbb{Q}_p^\times$. As in Remark 9, it follows that $(a,b)_p = 1$ if and only if $a \in \mathbb{Q}_p^\times$.

Case 2. $b \notin \mathbb{Q}_p^{\times 2}$

The proposition follows from the equivalence of the following four conditions :

$$\begin{aligned}
(a,b)_p = 1 &\Leftrightarrow \exists\,(x,y) \in \mathbb{Q}_p^2 \text{ such that } ax^2 + by^2 = 1 \quad \text{(Theorem 34)} \\
&\Leftrightarrow \exists\,(x,y,z) \in \mathbb{Q}_p^3, (x,y,z) \neq (0,0,0) \text{ such that } ax^2 + by^2 = z^2 \\
&\Leftrightarrow \exists\,(y,z) \in \mathbb{Q}_p^2 \text{ such that } a = z^2 - by^2 \quad \text{(box given in Theorem 34)} \\
&\Leftrightarrow a \in N_b(K_b^\times)
\end{aligned}$$

□

Corollary 8. *$N_b(K_b^\times) = b^\perp$, where the orthogonal is taken with respect to the hilbertian pairing*[29].

Corollary 9. *For every quadratic extension E of $\mathbb{Q}_p$, the subgroup $N_{E|\mathbb{Q}_p}(E^\times)$ of $\mathbb{Q}_p^\times$ is an open subgroup of index 2.*

2.7 Reciprocity Isomorphism

One should notice that Cayley tables in Corollary 7 are the same as the ones in Corollary 5 and Corollary 6 giving the values of the basic quadratic characters on the chosen basis of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, with the important exception of the $(2,2)$ entry $\lambda_4(p) = \lambda_p(-1)$. This phenomenon will get explained here as we will interpret the hilbertian symbol in terms of the *reciprocity isomorphism* for the maximal abelian extension of $\mathbb{Q}_p$ of exponent 2.

Theorem 36. *There is a unique bijection $E \mapsto \chi$ between the set $\mathcal{E}$ of quadratic extensions of $\mathbb{Q}_p$ and the set $\mathcal{Q}$ of quadratic characters of $\mathbb{Q}_p^\times$ such that $\ker(\chi) = N_{E|\mathbb{Q}_p}(E^\times)$. The induced map $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to \mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{Z}^\times)$ is an isomorphism of groups.*

Proof. Let p be an odd prime number. As seen in Definition 23, the field $\mathbb{Q}_p$ has three quadratic extensions, namely those obtained by adjoining $\sqrt{u}, \sqrt{-p}, \sqrt{-p \cdot u}$ (the reason for choosing $-p$ instead of p is that $(-p,p)_p = 1$ whereas $(p,p)_p = 1$ only when $\lambda_4(p) = 1$) where, we have any unit $u \in \mathbb{Z}_p^\times$ such that $\lambda_p(u) = -1$ can be chosen. From Corollary 5 we know that the group $\mathbb{Q}_p^\times$ has three quadratic characters, namely $\mu_p,\ \lambda_p,\ \mu_p\lambda_p$ (with the choice of p as a uniformiser of $\mathbb{Q}_p$).

For $p = 2$, as seen in Definition 23, the field $\mathbb{Q}_2$ has seven quadratic extensions, namely those obtained by adjoining

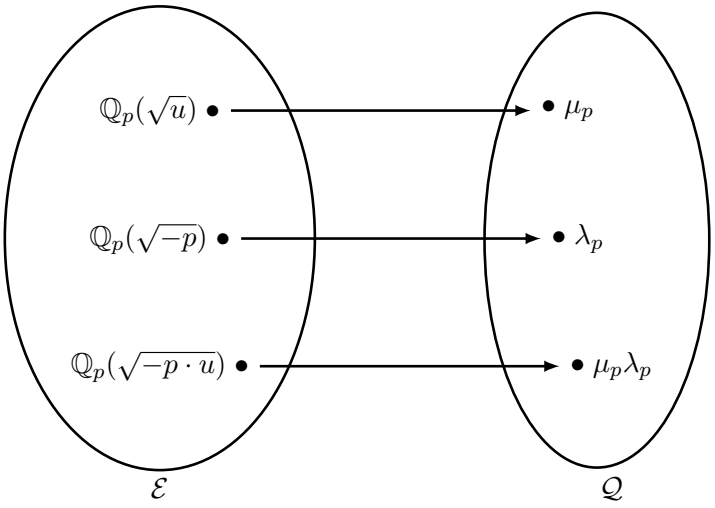
$$\sqrt{5}, \sqrt{-1}, \sqrt{-1 \cdot 5}, \sqrt{2}, \sqrt{2 \cdot 5}, \sqrt{-1 \cdot 2}, \sqrt{-1 \cdot 2 \cdot 5}$$

From Corollary 5 we know that the group $\mathbb{Q}_2^\times$ has seven quadratic characters, namely

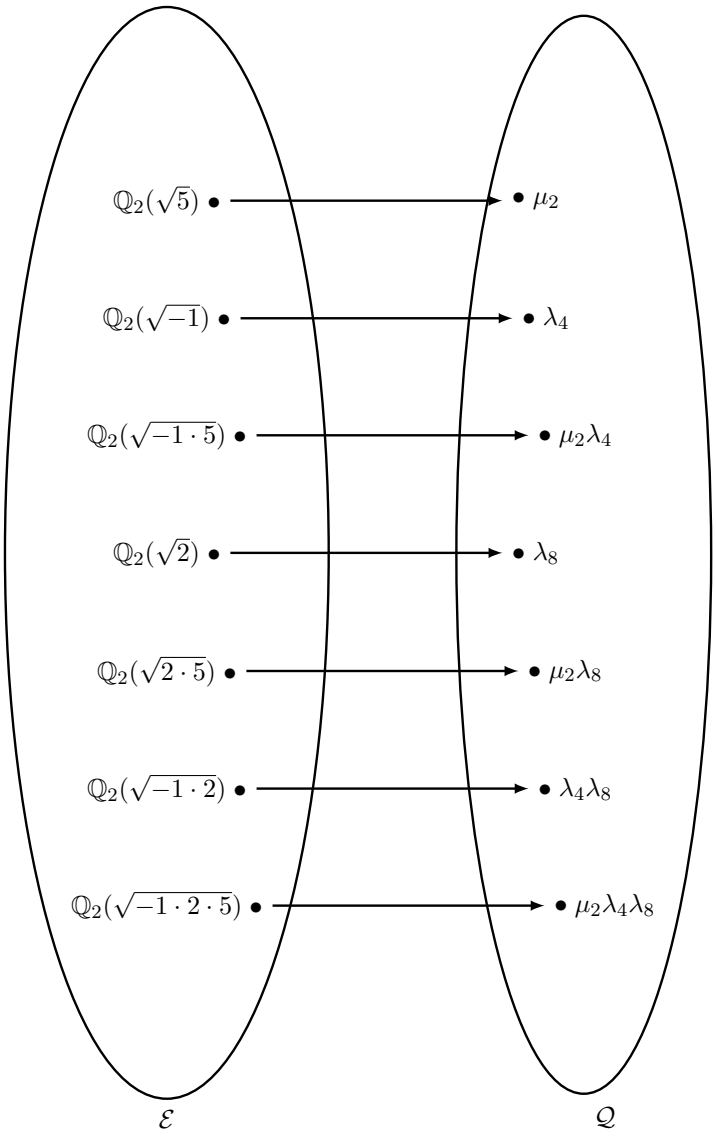
$$\mu_2,\ \ \lambda_4,\ \ \mu_2\lambda_4,\ \ \lambda_8,\ \ \mu_2\lambda_8,\ \ \lambda_4\lambda_8,\ \ \mu_2\lambda_4\lambda_8$$

We claim that the bijection is as given in Figure 2.1. This is simple to verify, since for each $E \in \mathcal{E}$ and corresponding $\chi \in \mathbb{Q}$ we just need to check that $\ker(\chi) = N_{E|\mathbb{Q}_p}(E^\times)$.

[29] Quadratic hilbertian symbol is a bilinear form (multiplicatively written) i.e. a function combining elements of two vector spaces to yield an element of third vector space and is linear in each of its arguments. Hilbertian pairing is reflexive since $(a,b)_p = 1$ implies $(b,a)_p = 1$ for all $a, b \in \mathbb{Q}_p$. For a reflexive bilinear form, a and b in $\mathbb{Q}p^\times$ will be orthogonal with respect to $(\ ,\ )_p$ if $(a,b)_p = 1$.



(a) When p is an odd prime



(b) When $p = 2$

Figure 2.1: The bijection between $\mathcal{E}$ and $\mathcal{Q}$ when p is an odd prime and when $p = 2$

.

Let's verify for all ten cases one by one.

Case 1. $E = \mathbb{Q}_p(\sqrt{u})$ and $\chi = \mu_p$

$\ker(\mu_p) = \left\{x \in \mathbb{Q}_p^\times \ : \ v_p(x) \in 2\mathbb{Z}\right\}$, hence $\ker(\mu_p) = p^{2\mathbb{Z}}\mathbb{Z}_p^\times$. Given $a \in \mathbb{Q}_p^\times$ we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_p}(E^\times) &\Leftrightarrow (a,u)_p = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow \lambda_p\left(u^{v_p(a)}\right) = 1 \\
&\Leftrightarrow (-1)^{v_p(a)} = 1 \quad (\because\ \lambda_p(u) = -1) \\
&\Leftrightarrow v_p(a) \in 2\mathbb{Z} \\
&\Leftrightarrow a \in \ker(\mu_p)
\end{aligned}$$

Case 2. $E = \mathbb{Q}_p(\sqrt{-p})$ and $\chi = \lambda_p$

$\ker(\lambda_p) = \left\{x \in \mathbb{Q}_p^\times \ : \ \lambda_p(t) = 1 \text{ for } x = p^m t\right\}$. Given $a \in \mathbb{Q}_p^\times$, such that $a = p^m t$ with $m \in \mathbb{Z}$ and $t \in \mathbb{Z}_p^\times$, we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_p}(E^\times) &\Leftrightarrow (a,-p)_p = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (p^m t,-p)_p = 1 \quad \text{(can't use Theorem 31)} \\
&\Leftrightarrow (p^m,-p)_p(t,-p)_p = 1 \quad \text{(Theorem 30)} \\
&\Leftrightarrow \lambda_p\left((-1)^m(-1)^m\right)(t,-p)_p = 1 \\
&\Leftrightarrow 1 \cdot \lambda_p(t) = 1 \quad \text{(Theorem 31)} \\
&\Leftrightarrow t \in \ker(\lambda_p)
\end{aligned}$$

Case 3. $E = \mathbb{Q}_p(\sqrt{-p \cdot u})$ and $\chi = \mu_p\lambda_p$

$\ker(\mu_p\lambda_p) = \left\{x \in \mathbb{Q}_p^\times \ : \ \mu_p(x) = \lambda_p(t) = \pm 1 \text{ for } x = p^m t\right\}$. Given $a \in \mathbb{Q}_p^\times$, we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_p}(E^\times) &\Leftrightarrow (a,-pu)_p = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (p^m t,-pu)_p = 1 \quad \text{(can't use Theorem 31)} \\
&\Leftrightarrow (p^m,-pu)_p(t,-pu)_p = 1 \quad \text{(Theorem 30)} \\
&\Leftrightarrow (p^m,-p)_p(p^m,u)_p(t,-p)_p(t,u)_p = 1 \quad \text{(Theorem 30)} \\
&\Leftrightarrow \lambda_p\left((-1)^m(-1)^m\right) \cdot (\lambda_p(u))^m \cdot \lambda_p(t) \cdot 1 = 1 \quad \text{(Theorem 31)} \\
&\Leftrightarrow 1 \cdot (-1)^m \cdot \lambda_p(t) = 1 \\
&\Leftrightarrow \begin{cases} m \in 2\mathbb{Z} \text{ and } \lambda_p(t) = 1 \\ m \notin 2\mathbb{Z} \text{ and } \lambda_p(t) = -1 \end{cases} \\
&\Leftrightarrow \mu_p(a) = \lambda_p(t) = \pm 1
\end{aligned}$$

Case 4. $E = \mathbb{Q}_2(\sqrt{5})$ and $\chi = \mu_2$

$\ker(\mu_2) = \left\{x \in \mathbb{Q}_2^\times \ : \ v_2(x) \in 2\mathbb{Z}\right\}$, hence $\ker(\mu_2) = 2^{2\mathbb{Z}}\mathbb{Z}_2^\times$. Given $a \in \mathbb{Q}_2^\times$ we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_2}(E^\times) &\Leftrightarrow (a,5)_2 = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (-1)^{\alpha_2 \cdot 0 + \alpha_1 \cdot 0 + \alpha_0 \cdot 1} = 1 \\
&\Leftrightarrow (-1)^{\alpha_0} = 1 \\
&\Leftrightarrow \alpha_0 = 0 \in \mathbb{Z}/2\mathbb{Z} \\
&\Leftrightarrow v_2(a) \in 2\mathbb{Z} \quad (\because\ v_2(a) \equiv \alpha_0 \pmod 2) \\
&\Leftrightarrow a \in \ker(\mu_2)
\end{aligned}$$

Case 5. $E = \mathbb{Q}_2(\sqrt{-1})$ and $\chi = \lambda_4$

$\ker(\lambda_4) = \left\{x \in \mathbb{Q}_2^\times \ : \ \lambda_4(t) = 1 \text{ for } x = 2^m t\right\}$. Given $a \in \mathbb{Q}_2^\times$ we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_2}(E^\times) &\Leftrightarrow (a, -1)_2 = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (-1)^{\alpha_2 \cdot 0 + \alpha_1 \cdot 1 + \alpha_0 \cdot 0} = 1 \\
&\Leftrightarrow (-1)^{\alpha_1} = 1 \\
&\Leftrightarrow \alpha_1 = 0 \in \mathbb{Z}/2\mathbb{Z} \\
&\Leftrightarrow a = 5^r 2^m \text{ for some } r \in \mathbb{N} \quad \text{(Corollary 6)} \\
&\Leftrightarrow a \in \ker(\lambda_4) \quad (\because \lambda_4(5) = 1)
\end{aligned}$$

Case 6. $E = \mathbb{Q}_2(\sqrt{-1 \cdot 5})$ and $\chi = \mu_2\lambda_4$

$\ker(\mu_2\lambda_4) = \left\{x \in \mathbb{Q}_2^\times \ : \ \mu_2(x) = \lambda_4(t) = \pm 1 \text{ for } x = 2^m t\right\}$. Given $a \in \mathbb{Q}_2^\times$, we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_2}(E^\times) &\Leftrightarrow (a, -5)_2 = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (-1)^{\alpha_2 \cdot 0 + \alpha_1 \cdot 1 + \alpha_0 \cdot 1} = 1 \\
&\Leftrightarrow \alpha_0 \equiv \alpha_1 \pmod 2 \\
&\Leftrightarrow a = 5^r (-1)^s 2^m \text{ for some } m \equiv s \pmod 2 \quad \text{(Corollary 6)} \\
&\Leftrightarrow \begin{cases} \mu_2(a) = -1, \quad \lambda_4(t) = \lambda_4\left(5^r \cdot (-1)^s\right) = -1 & \text{if both odd} \\ \mu_2(a) = 1, \quad \lambda_4(t) = \lambda_4\left(5^r \cdot (-1)^s\right) = 1 & \text{if both even} \end{cases} \\
&\Leftrightarrow \mu_2(a) = \lambda_4(t) = \pm 1
\end{aligned}$$

Case 7. $E = \mathbb{Q}_2(\sqrt{2})$ and $\chi = \lambda_8$

$\ker(\lambda_8) = \left\{x \in \mathbb{Q}_2^\times \ : \ \lambda_8(t) = 1 \text{ for } x = 2^m t\right\}$. Given $a \in \mathbb{Q}_2^\times$ we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_2}(E^\times) &\Leftrightarrow (a, 2)_2 = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (-1)^{\alpha_2 \cdot 1 + \alpha_1 \cdot 0 + \alpha_0 \cdot 0} = 1 \\
&\Leftrightarrow (-1)^{\alpha_2} = 1 \\
&\Leftrightarrow \alpha_2 = 0 \in \mathbb{Z}/2\mathbb{Z} \\
&\Leftrightarrow a = (-1)^r 2^m \text{ for some } r \in \mathbb{N} \quad \text{(Corollary 6)} \\
&\Leftrightarrow a \in \ker(\lambda_8) \quad (\because \lambda_8(-1) = 1)
\end{aligned}$$

Case 8. $E = \mathbb{Q}_2(\sqrt{2 \cdot 5})$ and $\chi = \mu_2\lambda_8$

$\ker(\mu_2\lambda_8) = \left\{x \in \mathbb{Q}_2^\times \ : \ \mu_2(x) = \lambda_8(t) = \pm 1 \text{ for } x = 2^m t\right\}$. Given $a \in \mathbb{Q}_2^\times$, we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_2}(E^\times) &\Leftrightarrow (a, 10)_2 = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (-1)^{\alpha_2 \cdot 1 + \alpha_1 \cdot 0 + \alpha_0 \cdot 1} = 1 \\
&\Leftrightarrow \alpha_0 \equiv \alpha_2 \pmod 2 \\
&\Leftrightarrow a = 5^r (-1)^s 2^m \text{ for some } r \equiv m \pmod 2 \quad \text{(Corollary 6)} \\
&\Leftrightarrow \begin{cases} \mu_2(a) = -1, \quad \lambda_8(t) = \lambda_8\left(5^r \cdot (-1)^s\right) = -1 & \text{if both odd} \\ \mu_2(a) = 1, \quad \lambda_8(t) = \lambda_8\left(5^r \cdot (-1)^s\right) = 1 & \text{if both even} \end{cases} \\
&\Leftrightarrow \mu_2(a) = \lambda_8(t) = \pm 1
\end{aligned}$$

Case 9. $E = \mathbb{Q}_2(\sqrt{-1 \cdot 2})$ and $\chi = \lambda_4\lambda_8$

$\ker(\lambda_4\lambda_8) = \{x \in \mathbb{Q}_2^\times \ : \ \lambda_4(t) = \lambda_8(t) = \pm 1 \text{ for } x = 2^m t\}$. Given $a \in \mathbb{Q}_2^\times$, we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_2}(E^\times) &\Leftrightarrow (a,-2)_2 = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (-1)^{\alpha_2\cdot 1+\alpha_1\cdot 1+\alpha_0\cdot 0} = 1 \\
&\Leftrightarrow \alpha_1 \equiv \alpha_2 \pmod 2 \\
&\Leftrightarrow a = 5^r(-1)^s 2^m \text{ for some } r \equiv s \pmod 2 \quad \text{(Corollary 6)} \\
&\Leftrightarrow \begin{cases} \lambda_4(t) = -1, \quad \lambda_8(t) = -1 & \text{if both odd} \\ \lambda_4(t) = 1, \quad \lambda_8(t) = 1 & \text{if both even} \end{cases} \\
&\Leftrightarrow \lambda_4(t) = \lambda_8(t) = \pm 1
\end{aligned}$$

Case 10. $E = \mathbb{Q}_2(\sqrt{-1\cdot 2\cdot 5})$ and $\chi = \mu_2\lambda_4\lambda_8$

$\ker(\mu_2\lambda_4\lambda_8) = \{x \in \mathbb{Q}_2^\times \ : \ \mu_2\lambda_4\lambda_8(x) = \mu_2(x)\lambda_4(t)\lambda_8(t) = 1 \text{ for } x = 2^m t\}$.
Given $a \in \mathbb{Q}_2^\times$, such that $a = 5^r(-1)^s 2^m$ for some $r, s \in \mathbb{N}$, then we have

$$\begin{aligned}
a \in N_{E|\mathbb{Q}_2}(E^\times) &\Leftrightarrow (a,-10)_2 = 1 \quad \text{(Theorem 35)} \\
&\Leftrightarrow (-1)^{\alpha_2\cdot 1+\alpha_1\cdot 1+\alpha_0\cdot 1} = 1 \\
&\Leftrightarrow \alpha_0+\alpha_1+\alpha_2 \in 2\mathbb{Z} \\
&\Leftrightarrow \begin{cases} r \equiv s \equiv m \equiv 0 \pmod 2 \\ m \equiv s \equiv 1 \pmod 2,\ r \equiv 0 \pmod 2 \\ s \equiv r \equiv 1 \pmod 2,\ m \equiv 0 \pmod 2 \\ m \equiv r \equiv 1 \pmod 2,\ s \equiv 0 \pmod 2 \end{cases} \\
&\Leftrightarrow \begin{cases} \mu_2(a) = \lambda_4(t) = \lambda_8(t) = 1 \\ \mu_2(a) = -1,\ \lambda_4(t) = -1,\ \lambda_8(t) = 1 \\ \mu_2(a) = 1,\ \lambda_4(t) = -1,\ \lambda_8(t) = -1 \\ \mu_2(a) = -1,\ \lambda_4(t) = 1,\ \lambda_8(t) = -1 \end{cases} \\
&\Leftrightarrow \mu_2\lambda_4\lambda_8(x) = 1
\end{aligned}$$

From Definition 23 we know that $\mathcal{E}$ forms the basis of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ and from Corollary 5 and Corollary 6 we know that $\mathcal{Q}$ forms the basis of $\mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{Z})$. Thus we get a bijection $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to \mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{Z}^\times)$, and it's easy to see that this mapping is a morphism. Hence this is an isomorphism. □

Corollary 10. *There exist a group isomorphism between* $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ *and* $\mathrm{Hom}(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}, \mathbb{Z}^\times)$.

Proof. This follows from the previous theorem since $\mathrm{Hom}(\mathbb{Q}_p^\times, \mathbb{Z}^\times) = \mathrm{Hom}(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}, \mathbb{Z}^\times)$ because all squares in $\mathbb{Q}_p^\times$ must map to 1 in $\mathbb{Z}^\times$. □

Remark 10. Following Remark 8 we can say that the unramfied quadratic character μ_p corresponds to $\mathbb{Q}_p(\sqrt{u})$ (for $p \neq 2$) and to $\mathbb{Q}_2(\sqrt{5})$ (for $p = 2$). These quadratic extensions will therefore be called *unramified* (over $\mathbb{Q}_p$). Note that $\mathbb{Q}_2(\sqrt{5})$ contains $\sqrt{-3}$ and hence a primitive 3-rd root of unity i.e. $\frac{-1+\sqrt{-3}}{2}$ and $\frac{-1-\sqrt{-3}}{2}$.

Definition 24 (Maximal abelian extension of exponent 2)**.** M is called the maximal abelian extension of exponent 2 if it is the compositum of all quadratic extensions of $\mathbb{Q}_p$.

Remark 11. $M = \mathbb{Q}_p(\sqrt{u}, \sqrt{-p})$ if $p \neq 2$ and $M = \mathbb{Q}_2(\sqrt{5}, \sqrt{-1}, \sqrt{2})$ for $p = 2$.

Definition 25 (Pairing)**.** Let R be a commutative ring with unity, and M, N and L be three R-modules. A pairing is any R-bilinear map $e : M \times N \to L$.

Remark 12. A pairing can also be considered as an R-linear map $\Phi : M \to \mathrm{Hom}_R(N, L)$, which matches the first definition by setting $\Phi(m)(n) := e(m, n)$.

Definition 26 (Perfect pairing)**.** A pairing is called perfect if the above map Φ is an isomorphism of R-modules.

Definition 27 (Kummerian pairing)**.** For $G = \mathrm{Gal}(M|\mathbb{Q}_p)$, the perfect pairing $\langle\ ,\ \rangle_p : G \times (\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}) \to \mathbb{Z}^\times$ given by $\langle \sigma, b\rangle = \frac{\sigma(\sqrt{b})}{\sqrt{b}}$ for every $\sigma \in G$ and every $b \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ is called kummerian pairing.

Theorem 37 (Reciprocity isomorphism[30])**.** *Let $G = \mathrm{Gal}(M|\mathbb{Q}_p)$. There is a unique isomorphism[31] $\rho_M : \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to G$ such that for every quadratic extension E of $\mathbb{Q}_p$ (contained in M), the kernel of the composite map $\rho_E : \mathbb{Q}_p^\times \to \mathrm{Gal}(E|\mathbb{Q}_p)$ is $N_{E|\mathbb{Q}_p}(E^\times)$.*

Proof. We have the perfect pairing $\langle\ ,\ \rangle_p : G \times (\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}) \to \mathbb{Z}^\times$, so we have the canonical isomorphism $G \to \mathrm{Hom}(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}, \mathbb{Z}^\times)$. In Corollary 10 we have established the isomorphism $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to \mathrm{Hom}(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}, \mathbb{Z}^\times)$, and hence we get an isomorphism $\rho_M : \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \to G$.

Now we will show that ρ_M has the stated property. This follows from the fact that when we identify these two groups using ρ_M, the kummerian pairing $\langle\ ,\ \rangle_p$ gets converted into the hilbertian pairing $(\ ,\ )_p$, and we have shown in Theorem 35 that $(a, b)_p = 1$ if and only if a is a norm from the extension $\mathbb{Q}_p(\sqrt{b})$. □

Remark 13. Whenever K contains a primitive n-th root of unity, we would combine the reciprocity isomorphism with the kummerian pairing on $G \times (K^\times/K^{\times n})$ with values in the group of n-th roots of unity, to get the hilbertian symbol $\left(\frac{\ ,\ }{K}\right)_n$ (which was simply denoted $(\ ,\ )_p$ for $n = 2$ and $K = \mathbb{Q}_p$). This is not at all easy, even for $n = p$.

Now to explain the phenomenon remarked at the beginning of this section, note that the reciprocity isomorphism ρ_M gives back the bijection $E \mapsto \chi$ of Theorem 36. Indeed, quadratic extensions of $\mathbb{Q}_p$ correspond to quadratic characters of G and hence (applying ρ_M^{-1}) to quadratic characters of $\mathbb{Q}_p^\times$. We can illustrate what we have achieved using following diagram:

$$\begin{array}{ccc} \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} & \xrightarrow{\sim} & \mathrm{Gal}(M|\mathbb{Q}_p) \\ \updownarrow & & \updownarrow \quad \text{Fundamental Theorem of Galois Theory} \\ \mathcal{Q} & \xrightarrow{\sim} & \mathcal{E} \end{array}$$

One of the main results of the theory of *abelian extensions of local fields* says that for every local field K (of which $\mathbb{Q}_p$ is the first example) and for every $n > 0$, there is a unique isomorphism $\rho : K^\times/K^{\times n} \to \mathrm{Gal}(M|K)$, where M is the maximal abelian extension of K of exponent dividing n, such that for every abelian extension $E \mid K$ of exponent dividing n, the kernel of the resulting composite map $K^\times \to \mathrm{Gal}(E|K)$ is $N_{E|K}(E^\times)$ (and such that uniformisers correspond to the canonical generator σ of the residual extension, as opposed to its inverse σ^{-1}). We have proved the case $K = \mathbb{Q}_p$, $n = 2$ (and didn't need to worry about uniformisers because an automorphism of order 2 is its own inverse).[2]

[30] Prof. Dalawat calls this "minor miracle"[2, 14].

[31] As an $\mathbb{F}_2$-space, the dimension of G is 2 if $p \neq 2$ and 3 if $p = 2$, so there are many isomorphisms of G with the group $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, which has the same $\mathbb{F}_2$-dimension. Among these isomorphisms this one is very special.

Conclusion

Apart from looking at various reciprocity ideas, using p-adic numbers we have achived an understanding of how to approach the general problem. In words of Prof. Dalawat[2]

> ...What we have achieved might not seem much, but it is rare to be able to compute explicitly, for a given galoisian extension M of a field K, a set of elements $S \subset M$ such that $M = K(S)$, the group $G = \mathrm{Gal}(M|K)$, and $\sigma(s)$ for every $\sigma \in G$ and $s \in S$. This is what we have done for $K = \mathbb{Q}_v$ and M the maximal abelian extension of exponent 2. ...
>
> ...It is a minor miracle — in my view — that whereas ρ_M is uniquely determined by imposing the condition $\ker(\rho_E) = N_{E|\mathbb{Q}_p}(E^\times)$ on any two (resp. three for $p = 2$) of the three (resp. seven) quadratic extensions E whose compositum is M, this condition is automatically satisfied by the remaining quadratic extension(s). In other words, ρ_M is independent of the choice of bases. ...
>
> ...It is now clear what we should do if we want to understand higher reciprocity laws. We should first understand for each $\mathbb{Q}_p$ and for its finite extensions K, and for every integer $n > 0$, the group $\mathrm{Gal}(M|K)$ of K-automorphisms of the maximal abelian extension M of K of exponent dividing n. It will turn out that there is a canonical (up to sign) reciprocity isomorphism $K^\times/K^{\times n} \to \mathrm{Gal}(M|K)$, so the group $\mathrm{Gal}(M|K)$, which in some sense is external to K, can be understood in terms of the group $K^\times$. ...

Using this formulation, Hilbert stated and proved the main theorem of *classical reciprocity laws*. The only shortcoming of this law is that it is applicable only to those number fields which contain a primitive m-th root of unity[14]. Later, Hilbert also conjectured (Hilbert's ninth problem) a higher-power reciprocity law over any number field. That conjecture was tackled by Hasse, Takagi, and finally Artin, who stated a general reciprocity law[9]. This general reciprocity law removes the restriction of presence of relevant roots of unity in the number field under discussion. From Artin's reciprocity law, all other reciprocity laws can be derived[7].

The study of reciprocity laws led to class field theory. The abelian extensions of $\mathbb{Q}$ are easy to describe because of the Kronecker-Weber theorem[32] asserts that they are all contained in fields generated by roots of unity. This explains the role of the roots of unity in the classical reciprocity laws. But, as Prof. Kedlaya says[9]

> ...However, describing the Abelian extensions of an arbitrary number field K is somewhat harder. They can at least be classified in terms of the structure of the field K itself; this is what is commonly referred to as class field theory. However, explicitly specifying generators of the Abelian extensions of K (Hilbert's twelfth problem) remains mostly unsolved, except in some special cases. ...

[32] My previous report[16] ended just before we could introduce this theorem, but we illustrated this idea in specific examples of number fields.

Appendix A

Formal Power Series

Let p be a prime number. Let k a finite extension of the field $\mathbb{F}_p$, and $B = k[t]$ where t is an indeterminate. For every $n > 0$, we have the finite k-algebra $B_n = B/t^nB$ with q^n elements, where $q = p^f$ is the cardinality of k, and a surjective morphism of k-algebras $\varphi_n : B_{n+1} \to B_n$, with kernel t^nB_{n+1}, so we have the inverse system $(\varphi_n : B_{n+1} \to B_n)_{n>0}$ of *finite discrete k-algebras* whose projective limit is the profinite k-algebra $\mathfrak{o} = k[[t]]$. The elements of this ring are formal power series $\sum_{n\in\mathbb{N}} b_n t^n$, where $b_n \in k$. We observe that the field of fractions $K = k((t))$ of $\mathfrak{o}$ such that $K = \mathfrak{o}[t^{-1}]$, is similar to the field of fractions $\mathbb{Q}_p$ of $\mathbb{Z}_p$.

#	Statement	p-adic version
1	The ideal $\mathfrak{t} = t\mathfrak{o}$ is the unique maximal ideal of the k-algebra $\mathfrak{o}$.	Theorem 4
2	Every $a \neq 0$ in $\mathfrak{o}$ can be uniquely written as $a = t^n u_a$ ($n \in \mathbb{N}$, $u_a \in \mathfrak{o}^\times$).	Theorem 5
3	For every $a \neq 0$ in $\mathfrak{o}$, put $v_t(a) = n$ if $a = t^n u$ for some $u \in \mathfrak{o}^\times$. Also put $v_t(0) = +\infty$.[1]	Definition 6
4	$v_t(a) = 0 \Leftrightarrow a \in \mathfrak{o}^\times$, and the ideal $t\mathfrak{o}$ consists of $a \in \mathfrak{o}$ such that $v_t(a) > 0$.	Remark 5
5	Every ideal $\mathfrak{a} \neq 0$ of $\mathfrak{o}$ is generated by t^n for some $n \in \mathbb{N}$, so that $\mathfrak{a} = \mathfrak{t}^n$.	Theorem 7
6	For every $n > 0$, let $U_n = \ker(\mathfrak{o}^\times \to B_n^\times)$, so that $U_n = 1 + \mathfrak{t}^n$ and $\mathfrak{o}^\times/U_n = B_n^\times$; in particular $\mathfrak{o}^\times/U_1 = k^\times$.	Definition 14
7	$\mathfrak{o}^\times = k^\times \cdot U_1$.	Theorem 18
8	Suppose that $p \neq 2$. For every $x \in U_1$, there is a unique $y \in U_1$ such that $x = y^2$.	Lemma 5
9	If $p \neq 2$, then there is a unique isomorphism $\lambda_k : k^\times/k^{\times 2} \to \mathbb{Z}^\times$, and the natural map $\mathfrak{o}^\times/\mathfrak{o}^{\times 2} \to k^\times/k^{\times 2}$ is also an isomorphism.	Theorem 15
10	Every $a \neq 0$ in K can be uniquely written as $a = t^n u_a$ ($n \in \mathbb{Z}$, $u_a \in \mathfrak{o}^\times$).	Theorem 25
11	If we put $v_t(a) = n$ for $a = t^n u_a$, then v_t is a surjective morphism of groups $K^\times \to \mathbb{Z}$ satisfying $v_t(a + b) \geq \inf(v_t(a), v_t(b))$ with equality if $v_t(a) \neq v_t(b)$ and the convention that $v_t(0) = +\infty$.	Definition 17
12	Suppose that $p \neq 2$, and choose $u \in k^\times$ such that $\lambda_k(u) = -1$. Then the quotient group $K^\times/K^{\times 2}$ consists of $\bar{1}, \bar{u}, \bar{t}, \bar{u}\bar{t}$.	Theorem 28
13	For every prime p, the morphism $\mu_t(x) = (-1)^{v_t(x)}$ is a quadratic character of $K^\times$; we call it the *unramified* quadratic character.	Definition 21

[1] Note that $v_t(p) = +\infty$ whereas we had $v_p(p) = 1$ in the case of $\mathbb{Q}_p$.

14	The retraction $x \mapsto t^{-v_t(x)}$ of the inclusion $\mathfrak{o}^\times \to K^\times$, allows us to view quadratic characters of $\mathfrak{o}^\times$ as ramified quadratic characters of $K^\times$	Remark 8
15	For $p \neq 2$, the quadratic characters μ_t, λ_k constitute a basis of the $\mathbb{F}_2$-space $\mathrm{Hom}(K^\times, \mathbb{Z}^\times)$; their values on the basis $\bar{u}, \bar{t}$ of $K^\times/K^{\times 2}$ are given by the table $\begin{array}{c\|cc} & \bar{u} & \bar{t} \\ \hline \mu_t & 1 & -1 \\ \lambda_k & -1 & 1 \end{array}$	Corollary 5
16	If $p \neq 2$, the quadratic hilbertian symbol $(\ ,\ )_t : K^\times \times K^\times \to \mathbb{Z}^\times$ for $a, b \in K^\times$ is defined as $(a,b)_t = \lambda_k(\gamma_{a,b})$ where $\gamma_{a,b} = (-1)^{v_t(a)v_t(b)} a^{v_t(b)} b^{-v_t(a)} \in \mathfrak{o}^\times$.	Definition 22
17	For $a, b \in K^\times$ we have $(a,b)_t = (b,a)_t$; $(a,bc)_t = (a,b)_t(a,c)_t$; $(a,-a)_p = 1$.	Theorem 30
18	$(a,b)_t$ depends only on the classes of a, b modulo $K^{\times 2}$ in the sense that $(a,b)_t = (ac^2, b)_t$ for every $c \in K^\times$ and $(a,b)_t = (a, bd^2)_t$ for every $d \in K^\times$.	Remark 9
19	Let $a, b \in \mathfrak{o}^\times$, then $(a,b)_t = 1$ and $(a, tb)_t = \lambda_k(a)$.	Theorem 31
20	$(t,t)_t = \lambda_k(-1)$	Theorem 33
21	For every $p \neq 2$, the pairing $(\ ,\ )_t$ is invertible in the sense that its Caylet table $\begin{array}{c\|cc} (\ ,\ )_t & u & t \\ \hline u & 1 & -1 \\ t & -1 & \lambda_k(-1) \end{array}$ when expressed as matrices (with entries in $\mathbb{Z}^\times$) with respect to the given basis of $K^\times/K^{\times 2}$ is invertible (when viewed with entries in the field $\mathbb{F}_2$). Indeed, in $\mathbb{F}_2$, $\begin{vmatrix} 0 & 1 \\ 1 & * \end{vmatrix} = 1$ (here $*$ is some non-zero value)	Corollary 7
22	Let $a, b \in K^\times$. If $a + b = 1$, then $(a,b)_t = 1$.	Lemma 12
23	Suppose that $p \neq 2$ and let $a, b \in K^\times$. There exist $x, y \in K$ such that $ax^2 + by^2 = 1$ if and only if $(a,b)_t = 1$.	Theorem 34
24	Let $b \in K^\times$, and put $L_b = K(\sqrt{b})$, so that the degree $[L_b : K]$ equals 1 or 2 according as $b \in K^{\times 2}$ or $b \notin K^{\times 2}$ (still assuming $p \neq 2$). We have the norm homomorphism $N_b : L_b^\times \to K^\times$ which is the identity in case $L_b = K$ and sends $x + y\sqrt{b}$ $(x, y \in K)$ to $x^2 - by^2$ in case $[L_b : K] = 2$.	Definition 23
25	Suppose that $p \neq 2$ and let $a, b \in K^\times$. We have $(a,b)_t = 1$ if and only if $a \in N_b(L_b^\times)$.	Theorem 35
26	$N_b(L_b^\times) = b^\perp$, where the orthogonal is taken with respect to the hilbertian pairing.	Corollary 8
27	Suppose $p \neq 2$. For every quadratic extension E of K, the subgroup $N_{E\|K}(E^\times)$ of $K^\times$ is an open subgroup of index 2.	Corollary 9
28	If $p \neq 2$, there is a unique bijection $E \mapsto \chi$ between the set of quadratic extensions of K and the set of quadratic characters of $K^\times$ such that $\ker(\chi) = N_{E\|K}(E^\times)$. The induced map $K^\times/K^{\times 2} \to \mathrm{Hom}(K^\times, \mathbb{Z}^\times)$ is an isomorphism of groups.	Theorem 36
29	The unramfied quadratic character μ_t corresponds to $K(\sqrt{u})$. These quadratic extensions will therefore be called unramified (over K).	Remark 10
30	$M = K(\sqrt{u}, \sqrt{-t})$ if $p \neq 2$ is the maximal abelian extension of exponent 2	Remark 11

31	When $p \neq 2$, there is a unique isomorphism $\rho_M : K^\times/K^{\times 2} \to \mathrm{Gal}(M\|K)$ such that for every quadratic extension E of K (necessarily contained in M), the kernel of the composite map $\rho_E : K^\times \to \mathrm{Gal}(E\|K)$ is $N_{E\|K}(E^\times)$.	Theorem 37

Except for the proofs of # 1, # 2, # 8 and# 9, which take advantage of the fact that elements of $k[[t]]$ are just formal power series[2], proofs of all other statements can be obtained by just replacing p by t in their p-adic version.

Proof of # 1. As in p-adic case (Lemma 2), we have to show that if $a = a_0 + a_1 t + a_2 t^2 + \cdots$ is not in $t\mathfrak{o}$ (or equivalently if $a_0 \neq 0$), then $a \in \mathfrak{o}^\times$. Look for an a^{-1} of the form $b = b_0 + b_1 t + b_2 t^2 + \cdots$. Comparing the coefficients of t^n in the relation $ab = 1$ leads to $b_0 = a_0^{-1}$ (for $n = 0$) and recursively to

$$b_n = a_0^{-1}(-a_1 b_{n-1} - \cdots - a_{n-1} b_1 - a_n b_0)$$

for $n > 0$. Hence $a \in \mathfrak{o}^\times$. (So $\mathfrak{o}$ is a principal local ring like $\mathbb{Z}_p$.) □

Proof of # 2. Write $a = a_0 + a_1 t + a_2 t^2 + \cdots$. As $a \neq 0$, there is a smallest $n \in \mathbb{N}$ such that $a_n \neq 0$, and then $a = t^n u_a$, with $u_a = a_n + a_{n+1} t + a_{n+2} t^2 \cdots$. As $a_n \neq 0$, we have $u_a \in \mathfrak{o}^\times$ (from # 1), proving the statement. □

Proof of # 8. Let $x = 1 + x_1 t + x_2 t^2 + \cdots$ (with $x_i \in k$), and let us look for a square root y of x of the form $y = 1 + y_1 t + y_2 t^2 + \cdots$ (with $y_i \in k$). Equating the coefficients of t^n in the relation $y^2 = x$, we are led to the relations $x_1 = 2y_1$, $x_2 = 2y_2 + y_1^2$, $x_3 = 2y_3 + 2y_1 y_2$ and so on. Since $2 \in k^\times$, these equations can be solved recursively to get $y_1 = x_1/2$, $y_2 = (x_2 - y_1^2)/2$, $y_3 = (x_3 - 2y_1 y_2)/2$ and so on[3]. □

Proof of # 9. Let $q = \mathrm{Card}(k)$; we have $q = p^f$ for some $f > 0$. As $p \neq 2$, the order $q - 1$ of $k^\times$ is even. Recall also that the group $k^\times$ is cyclic, so the quotient $k^\times/k^{\times 2}$ is of order 2, and hence there is a unique isomorphism $\lambda_k : k^\times/k^{\times 2} \to \mathbb{Z}^\times$ of groups. Finally, the natural map $\mathfrak{o}^\times/\mathfrak{o}^{\times 2} \to k^\times/k^{\times 2}$ is also an isomorphism because $\mathfrak{o}^\times = k^\times U_1$ (from # 7) and $U_1 = U_1^2$ (from # 8). □

Remark. Just as in p-adic formulation $\mathbb{Z}_p^\times$ ($p \neq 2$) had the unique quadratic character λ_p, here $\mathfrak{o}^\times$ ($p \neq 2$) has the unique quadratic character λ_k. But $\mathbb{Z}_2^\times$ had three quadratic characters (namely λ_4, λ_8 and $\lambda_4\lambda_8$). But for $p = 2$, $\mathfrak{o}^\times$ has infinitely many quadratic characters since the $\mathbb{F}_2$-space $\mathfrak{o}^\times/\mathfrak{o}^{\times 2}$ is infinite. In fact, for every prime p, the $\mathbb{F}_p$-space $\mathfrak{o}^\times/\mathfrak{o}^{\times p}$ is infinite. We will not discuss the case when $p = 2$, since it requires the knowledge of *function fields*.

[2] We don't need something like Hensel's lemma in the proof of # 8.

[3] In general, $x_n = 2y_n + f_n(y_1, y_2, \ldots, y_{n-1})$ for some polynomial $f_n(Y_1, Y_2, \ldots, Y_{n-1})$ with coefficients in $\mathbb{F}_p$, so one can solve for y_n recursively to get $y_n = (x_n - f_n(y_1, y_2, \ldots, y_{n-1}))/2$.

Bibliography

[1] Dalawat, C. S. *Eight lectures on quadratic reciprocity*. Allahabad: Harish-Chandra Research Institute, 2014. http://arxiv.org/abs/1404.4918

[2] Dalawat, C. S. *Five Lectures on local quadratic reciprocity*. Allahabad: Harish-Chandra Research Institute, 2016.

[3] Marcus, D. A. *Number Fields*. New York: Springer-Verlag, 1977. http://dx.doi.org/10.1007/978-1-4684-9356-6

[4] Ash, A. and Gross, R. *Fearless Symmetry*. Princeton and Oxford: Princeton University Press, 2006. http://dx.doi.org/10.1515/9781400837779

[5] Berlekamp, E. *Algebraic Coding Theory.* (Revised Edition) World Scientific Publishing, 2015. https://doi.org/10.1142/9407

[6] Adhikari, S. D. "The Early Reciprocity Laws: From Gauss to Eisenstein." in *Cyclotomic Fields and Related Topics*, edited by S. D. Adhikari, S. A. Katre and D. Thakur, 55–74. Pune: Bhaskaracharya Pratishthana, 2000. http://www.bprim.org/sites/default/files/recipro1.pdf

[7] Shastri, P. "Reciprocity Laws: Artin-Hilbert" in *Cyclotomic Fields and Related Topics*, edited by S. D. Adhikari, S. A. Katre and D. Thakur, 175–183. Pune: Bhaskaracharya Pratishthana, 2000 . http://www.bprim.org/sites/default/files/rlmain.pdf

[8] Gouvêa, F. Q. "Local and Global in Number Theory." in *The Princeton Companion for Mathematics*, edited by T. Gowers, J. Barrow-Green and I. Leader, 243–246. Princeton and Oxford: Princeton University Press, 2008. http://dx.doi.org/10.1515/9781400830398.241

[9] Kedlaya, K. S. "From Quadratic Reciprocity to Class Field Theory." in *The Princeton Companion for Mathematics*, edited by T. Gowers, J. Barrow-Green and I. Leader, 718–720. Princeton and Oxford: Princeton University Press, 2008. Preprint available at http://kskedlaya.org/papers/pcm.pdf

[10] MacDuffee, C. C. "The p-adic Numbers of Hensel." *The American Mathematical Monthly* 45, no. 8 (1938), 500–508[4]. http://dx.doi.org/10.2307/2303739

[11] Wyman, B. F. "What is a Reciprocity Law?" *The American Mathematical Monthly* 79, no. 6 (1972), 571–586[5]. http://dx.doi.org/10.2307/2317083

[4] Please note that this is a very old article and the definition of valuation given in this article is now known as *p-adic absolute value*.

[5] A correction in the theorem in Section 6 (pp. 583) available as: Wyman, B. F. "Correction to "What Is a Reciprocity Law?" " *The American Mathematical Monthly* 80, no. 3 (1973), 281. http://dx.doi.org/10.2307/2318450. I would also like to point out that though the article introduces nice ideas, has some more typos. For example, on pp. 582 the basis set given doesn't include x.

[12] Cox, D. A. "Quadratic Reciprocity: Its Conjecture and Application." *The American Mathematical Monthly* 95, no. 5 (1988), 442–448. https://dx.doi.org/10.2307/2322482

[13] Rozikov, U.A. "What are p-adic Numbers? What are they used for?" *Asia Pacific Mathematics Newsletter* 3, no. 4 (2013), 1–6. http://www.asiapacific-mathnews.com/03/0304/0001_0006.pdf

[14] Dalawat, C. S. "Classical Reciprocity Laws." *Asia Pacific Mathematics Newsletter* 4, no. 4 (2014), 5–9. http://www.asiapacific-mathnews.com/04/0404/0005_0009.pdf

[15] Korpal, G. "Diophantine Equations." *Summer Internship Project Report*, guided by Prof. S. A. Katre (18 May 2015 – 16 June 2015)

[16] Korpal, G. "Number Fields." *Summer Internship Project Report*, guided by Prof. Ramesh Sreekantan (1 June 2016 – 31 July 2016)

Prepared in LaTeX 2_ε by Gaurish Korpal