LOCAL CLASS FIELD THEORY OVER $\mathbb{Q}_p$

CAMERON FRANC

Abstract. This note provides background on and an executive summary of local class field theory over $\mathbb{Q}_p$.

1. Infinite Galois Theory

Every field is contained in algebraic extensions that are algebraically closed. Such an extension is called an algebraic closure. Let $E$ be a field and fix an algebraic closure $\overline{E}$. If $L/K/E$ is a tower of Galois extensions, then restriction of automorphisms yields a surjective group homomorphism

$$\pi_{L/K} : \text{Gal}(L/E) \to \text{Gal}(K/E).$$

Since this map is literally given by functional restriction of field automorphisms, for any tower of fields $L/K/J/E$ one has that $\pi_{L/J} = \pi_{K/J} \circ \pi_{L/K}$. This is exactly like the system of surjective group homomorphisms

$$\pi_{n,m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}, \quad (n \geq m),$$

that were used to construct $\mathbb{Z}_p$.

Definition 1. The absolute Galois group of $\overline{E}/E$ is the profinite group

$$\text{Gal}(\overline{E}/E) := \lim_{\leftarrow}^{\text{K/Galois}} \text{Gal}(K/E).$$

This definition depends on the choice of $\overline{E}$. We examine exactly how it depends on this choice: let $E'/E$ denote another algebraic closure. It is a standard fact that $E$ and $E'$ are isomorphic over $E$, say via $f : \overline{E} \to E'$. If $K/E$ is Galois and contained in $\overline{E}$, then every embedding $K \hookrightarrow E'$ fixing $E$ pointwise has the same image, say $K' \subseteq E'$. We thus obtain group isomorphisms $\text{Gal}(K/E) \to \text{Gal}(K'/E)$ via $\sigma \mapsto f \circ \sigma \circ f^{-1}$. These isomorphisms are compatible with the projection maps defining $\text{Gal}(\overline{E}/E)$ and $\text{Gal}(E'/E)$, and so conjugation with $f$ induces an isomorphism of profinite groups $\text{Gal}(\overline{E}/E) \cong \text{Gal}(E'/E)$.

Elements of $\text{Gal}(\overline{E}/E)$ can be regarded as field automorphisms of $\overline{E}$ fixing $E$ pointwise. Let $(\sigma_K) \in \text{Gal}(\overline{E}/E)$ denote a compatible family of Galois automorphisms $\sigma \in \text{Gal}(K/E)$, where $K$ ranges over the finite Galois extensions $K/E$ in $\overline{E}$. Each $x \in \overline{E}$ is contained in the splitting field of its minimal polynomial over $E$, which is some finite Galois extension $K/E$ inside $\overline{E}$. Define $\sigma(x) = \sigma_K(x)$. One can use the compatibility of $(\sigma_K)$ under restriction to show that $\sigma$ is a field automorphism.

Galois theory extends to $\text{Gal}(\overline{E}/E)$, but one must take the topology into account.

Theorem 2 (Infinite Galois theory). The maps $K/E \mapsto \text{Gal}(\overline{E}/K)$, $H \mapsto (\overline{E})^H$, define an inclusion reversing bijection between the algebraic extensions of $E$ contained in $\overline{E}$ and
the closed subgroups of $\text{Gal}(\mathcal{E}/E)$. Moreover, $K/E$ is Galois if and only if $\text{Gal}(\mathcal{E}/K)$ is a normal subgroup of $\text{Gal}(\mathcal{E}/E)$ and in this case

$$\text{Gal}(K/E) \cong \frac{\text{Gal}(\mathcal{E}/E)}{\text{Gal}(\mathcal{E}/K)}.$$ 

**Remark 3.** When defining $\text{Gal}(\mathcal{E}/E)$ we only needed the property that $\mathcal{E}/E$ is Galois in order to get a group that is well-defined up to isomorphism. One can define $\text{Gal}(K/E)$ as a profinite group for any Galois extension, and the statements of Galois theory remain true for any such group.

A class field theory should describe the algebraic extensions (equivalently, the absolute Galois group) of a field intrinsically in terms of the base field. Although this is presently too much to ask for in complete generality, number theorists have had great success in understanding the abelian extensions of global and local fields. Since the compositum of two abelian extensions of any given field is always another abelian extension, any algebraic closure ${\overline{E}}/E$ contains a largest abelian extension $E^{ab}/E$. Note that $\text{Gal}(E^{ab}/E) \cong \text{Gal}(\mathcal{E}/E)/\text{Gal}(E/E^{ab})$ by Galois theory.

## 2. Finite fields

If $F/F_p$ is a finite extension, then $F$ is a finite dimensional $F_p$-vector space and hence contains $p^n$ elements for some $n \geq 1$. In fact, for each prime power $q = p^n$ there is a unique (up to isomorphism) field of size $q$. Denoted $F_q$, it is defined to be the splitting field of $X^q - X$ inside an algebraic closure $\overline{F}_p/F_p$. In particular, $F_q/F_p$ is a Galois extension. The multiplicative group $F_q^\times$ is cyclic, generated by a primitive $(q-1)$th root of unity $\zeta \in F_q$. The Frobenius automorphism $\text{Frob}_p \in \text{Gal}(F_q/F_p)$ is defined by $\text{Frob}_p(x) = x^p$. If $x \in F_q$ is a primitive element, then $x^q = x$, but for $1 \leq m < n$ one has that $x^{p^m} \neq x$. It follows that $\text{Frob}_p$ has exact order $n$. Since $[F_q:F_p] = n$, we see that $\text{Frob}_p$ must generate the Galois group $\text{Gal}(F_q/F_p)$. Hence $F_q/F_p$ is a cyclic Galois extension of degree $n$.

Given another prime power $q' = p^{n'}$, one has that $F_q \subseteq F_{q'}$ if and only if $n | m$. The Frobenius automorphism $\text{Frob}_{p'}$ of $F_{q'}$ restricts to that of $F_q$. It follows that the maps $\text{Frob}_p \mapsto 1$ define a compatible system of group isomorphisms $\text{Gal}(F_q/F_p) \cong \hat{Z}/n\hat{Z}$, and thus yield an isomorphism of profinite groups

$$\text{Gal}(\overline{F}_p/F_p) = \lim_{\text{n} | \text{m}} \text{Gal}(F_{p^n}/F_p) \cong \lim_{\text{n} | \text{m}} \hat{Z}/n\hat{Z}.$$ 

The rightmost group is often denoted $\hat{Z}$ and called $\text{ZEE-HAT}$ (or $\text{ZED-HAT}$). One can use the Chinese remainder theorem to prove that $\hat{Z} \cong \prod_{\ell} \hat{Z}_\ell$, where the product is over all prime numbers $\ell$.

## 3. Extensions of $Q_p$

Let $L/Q_p$ denote a finite (hence algebraic) extension of degree $n$. One can show that the $p$-adic valuation $v_p$ extends uniquely to a valuation $v$ on $L$ for which $L$ is complete. Assuming this, it is easy to deduce a formula for the putative valuation: for simplicity first suppose that $L/Q_p$ is Galois. Then if $\sigma \in \text{Gal}(L/Q_p)$, the valuation $v \circ \sigma$ also extends $v_p$ and hence by the assumed uniqueness of such a valuation, $v = v \circ \sigma$. 


But then we deduce that for any \( x \in L \),
\[
v_p(N_{L/Q_p}(x)) = v(N_{L/Q_p}(x)) = v \left( \prod_{\sigma \in \mathrm{Gal}(L/Q_p)} \sigma(x) \right) = \sum_{\sigma \in \mathrm{Gal}(L/Q_p)} v(\sigma(x)) = n v(x).
\]
Thus, if there exists a unique extension of \( v_p \) to \( L/Q_p \), then it must be given by the formula
\[
v(x) = \frac{1}{[L:Q_p]} v_p \left( N_{L/Q_p}(x) \right).
\]
To prove the uniqueness of such an extension one can argue that any two norms on a finite dimensional vector space over a complete field are equivalent in a precise sense, and in particular they induce the same (complete) topology on \( L \). Then one can use the multiplicative structure of \( L \) to argue that two valuations that induce the same topology on the field \( L \), and which agree on \( Q_p \), must be identical. Finally, one must show that equation (1) does in fact define a valuation on \( L \).

Since \( v_p \) tells how many times \( p \) divides a \( p \)-adic number, it takes values in \( \mathbb{Z} \). Note that the presence of the denominator in (1) seems to indicate that this will fail to be true for extensions. In fact, it frequently happens that the extension of \( v_p \) to a finite extension \( L/Q_p \) remains \( \mathbb{Z} \)-valued:

**Example 4.** Let \( p \) be a prime congruent to 3 mod 4, so that \(-1\) is not square mod \( p \). By reducing mod \( p \) one deduces that \( Q_p \) does not contain a primitive fourth root of unity. Let \( L = Q_p(\zeta) \) where \( \zeta \) is a primitive 4th root of unity. A generic element of \( L \) has the form \( a + b\zeta \) for \( a, b \in Q_p \), and the conjugate of \( \zeta \) is \(-\zeta \). Thus \( N_{L/Q_p}(a + b\zeta) = a^2 + b^2 \) and hence by (1),
\[
v(a + b\zeta) = \frac{v_p(a^2 + b^2)}{2}.
\]
Suppose that \( a \) and \( b \) are integers. In elementary number theory one learns that a positive integer can be expressed as a sum of squares if and only if all primes congruent to 3 mod 4 that divide it do so to an even power. Hence \( v_p(a^2 + b^2) \) is even for \( a \) and \( b \) integers. But then, by density of the integers in the \( p \)-adic integers, \( v_p(a^2 + b^2) \) is even for all \( a \) and \( b \in Z_p \) (Proof: the \( p \)-adic valuation is a continuous mapping into \( R \)). One deduces the result for \( a, b \in Q_p \) by rescaling. Thus, the extension of \( v_p \) to \( Q_p(\zeta) \) is \( \mathbb{Z} \)-valued.

We henceforth write the extension of \( v_p \) to a finite extension of \( Q_p \) also as \( v_p \).

**Definition 5.** A finite extension \( L/Q_p \) is said to be **unramified** if the unique extension of the \( p \)-adic valuation to \( L \) is \( \mathbb{Z} \)-valued. Otherwise \( L/Q_p \) is said to be **ramified**.

**Remark 6.** It is important to note that even if the extension of \( v_p \) to a finite algebraic extension is not \( \mathbb{Z} \)-valued, the value group is always a discrete subgroup of \( R \).

**Example 7.** Let \( L = Q_p(\pi) \) where \( \pi^2 = p \). Then \( 1 = v_p(p) = 2 v_p(\pi) \) shows that \( v_p(\pi) = 1/2 \). So \( L/Q_p \) is ramified. In this case the value group is \( (1/2) \mathbb{Z} \).

**Example 8.** Let \( p \) denote an odd prime. Let \( L = Q_p(\zeta) \) where \( \zeta \) is a primitive \( p \)th root of unity. One has \( v_p(\zeta) = 0 \), but this does not imply that \( L/Q_p \) is unramified. Consider \( \pi = 1 + \zeta \). We have that \((\pi - 1)^p = 1\), which implies that the minimal polynomial of
\[ \pi \text{ over } \mathbb{Q}_p \text{ is the Eisenstein polynomial} \]

\[ \sum_{i=0}^{p-1} (-1)^i \binom{p}{i} X^{p-1-i}. \]

Hence \( N_{L/\mathbb{Q}_p}(\pi) = (-1)^{p-1}p \) (the constant term of the polynomial above), and we see that \( v_p(\pi) = v_p(p)/(p-1) = 1/(p-1) \). So \( L/\mathbb{Q}_p \) is ramified.

**Definition 9.** Let \( L/\mathbb{Q}_p \) denote a finite extension. The **ramification index** of \( L \) is the integer \( e_L := [v_p(L^\times) : \mathbb{Z}] \). An element \( \pi \in L \) is said to be a **uniformizer** if \( v_p(\pi) = 1/e_L \).

**Remark 10.** Equation (1) implies that \( e_L \leq [L : \mathbb{Q}_p] \).

**Definition 11.** A finite extension \( L/\mathbb{Q}_p \) is said to be **totally ramified** if \( e_L = [L : \mathbb{Q}_p] \).

The unit ball \( \mathcal{O}_L \) in \( L \) is a Dedekind principal ideal domain, so that one can write \( p\mathcal{O}_L = (\pi)^e \) for a prime element \( \pi \) of \( L \) and a unique integer \( e \geq 1 \). One can show that \( e = e_L \) and \( \pi \) is a uniformizer for \( L/\mathbb{Q}_p \) (conversely, every uniformizer is a prime element of \( \mathcal{O}_L \)). This gives an algebraic description of ramification that agrees with the definition in algebraic number theory and algebraic geometry. There is also a useful algebraic interpretation of unramified extensions.

**Definition 12.** Let \( L/\mathbb{Q}_p \) be a finite extension and let \( \pi \in L \) be a uniformizer. The **residue field** of \( L \) is the field \( \kappa(L) := L/(\pi) \).

The residue field is a finite extension of \( \mathbb{F}_p \). It is well-defined because any two uniformizers define the same prime ideal, and to see that \( (\pi) \) is a maximal ideal for \( \pi \) a uniformizer, note at least one of the following two things:

1. The unit ball \( \mathcal{O}_L \) is a Dedekind domain, hence all nonzero primes are maximal;
2. The valuation of \( L \) is discrete, and \( \pi \) is defined to have minimal positive valuation. Things that properly divide \( \pi \) must have smaller valuation, hence the only things that properly divide \( \pi \) are the things of valuation 0. But these are the units in \( \mathcal{O}_L \). Hence \( (\pi) \) is maximal.

**Definition 13.** Let \( L/\mathbb{Q}_p \) denote a finite extension. The **residue degree** of \( L/\mathbb{Q}_p \) is the integer \( f_L := [\kappa(L) : \mathbb{F}_p] \).

**Remark 14.** Since a basis for \( L/\mathbb{Q}_p \) (scaled to be units in \( \mathcal{O}_L \)) reduces mod \( \pi \) to a spanning set for \( \kappa(L) \), it follows that \( f_L \leq [L : \mathbb{Q}_p] \).

The next proposition summarizes some of the main properties about ramification and unramified extensions.

**Proposition 15.** Let \( L/\mathbb{Q}_p \) denote a finite extension.

1. \( L/\mathbb{Q}_p \) is unramified if and only if \( f_L = [L : \mathbb{Q}_p] \).
2. One has \( [L : \mathbb{Q}_p] = e_L f_L \). Hence \( L/\mathbb{Q}_p \) is totally ramified if and only if \( f_L = 1 \).
3. Assume that \( K/\mathbb{Q}_p \) is a finite extension such that \( L \) and \( K \) are contained in a common field. If \( L \) and \( K \) are both unramified, then so is the compositum \( LK/\mathbb{Q}_p \).

The third part of this proposition implies that any finite extension \( L/\mathbb{Q}_p \) contains a largest unramified subextension \( K/\mathbb{Q}_p \). In this case \( f_L = f_K \) and \( e_K = 1 \).
**Example 16.** A compositum of totally ramified extensions need not be totally ramified: let \( p \) be an odd prime and choose an integer \( a \) coprime to \( p \) that is not square mod \( p \). Then \( \mathbb{Q}_p(\sqrt{p}) \) and \( \mathbb{Q}_p(\sqrt{ap}) \) are totally ramified and distinct with compositum

\[
\mathbb{Q}_p(\sqrt{p}, \sqrt{ap}) = \mathbb{Q}_p(\sqrt{p}, \sqrt{a}).
\]

The compositum visibly contains the extension \( \mathbb{Q}_p(\sqrt{a}) \), which is unramified by choice of \( a \). Since the residue field of \( \mathbb{Q}_p(\sqrt{a}) \) is larger than \( \mathbb{F}_p \), so too is the residue field of \( \mathbb{Q}_p(\sqrt{p}, \sqrt{a}) \), which means that this extension is not totally ramified.

One has the following rough classification of extensions of \( \overline{\mathbb{Q}}_p \).

**Theorem 17.** Let \( \overline{\mathbb{Q}}_p \) denote an algebraic closure of \( \mathbb{Q}_p \). Then \( \overline{\mathbb{Q}}_p \) contains exactly one unramified extension of degree \( n \) for every integer \( n \geq 1 \). The unramified extensions are generated by roots of unity of prime-to-\( p \) order. The ramified extensions can be generated by the root of an Eisenstein polynomial.

### 4. The local reciprocity law

We are now ready to discuss the reciprocity law for \( \mathbb{Q}_p \). If \( L/\mathbb{Q}_p \) is a finite extension of degree \( n \), then reduction mod a uniformizer yields an exact sequence of finite groups

\[
1 \to I_L \to \text{Gal}(L/\mathbb{Q}_p) \to \text{Gal}(\kappa(L)/\mathbb{F}_p) \to 1,
\]

where \( \text{Gal}(\kappa(L)/\mathbb{F}_p) \) is a cyclic group of some finite order. If \( L/\mathbb{Q}_p \) is unramified then, by definition, \( L/\mathbb{Q}_p \) and \( \kappa(L)/\mathbb{F}_p \) have the same degree. In this case \( I_L \) (the inertia subgroup) must be trivial and \( \text{Gal}(L/\mathbb{Q}_p) \cong \text{Gal}(\kappa(L)/\mathbb{F}_p) \). There thus exists a unique element \( \text{Frob}_p \in \text{Gal}(L/\mathbb{Q}_p) \) mapping to the Frobenius automorphism \( \text{Frob}_p \in \text{Gal}(\kappa(L)/\mathbb{F}_p) \). It is characterized by the property that \( x^p \equiv x \, (\text{mod} \, \pi_L) \) for all \( x \in O_L \), where \( \pi_L \) is a uniformizer for \( L \). This is called the Frobenius automorphism of the unramified extension \( L/\mathbb{Q}_p \).

**Theorem 18** (Local reciprocity law for \( \mathbb{Q}_p \)). There exists a unique homomorphism

\[
\phi: \mathbb{Q}_p^\times \to \text{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)
\]

satisfying the following properties:

1. For any \( L/\mathbb{Q}_p \) finite unramified, and for any \( x \in \mathbb{Z}_p^\times \), \( \phi(p) \) acts as Frobenius on \( L/\mathbb{Q}_p \) and \( \phi(x) \) acts trivially on \( L/\mathbb{Q}_p \);
2. For any finite abelian extension \( L/\mathbb{Q}_p \), the norm group \( N_{L/\mathbb{Q}_p}(L^\times) \) is an open subgroup of \( \mathbb{Q}_p^\times \) of finite index that is contained in the kernel of \( a \mapsto \phi(a)|_L \). Moreover, this induces an isomorphism of finite groups

\[
\phi_{L/K}: \mathbb{Q}_p^\times /N_{L/\mathbb{Q}_p}(L^\times) \to \text{Gal}(L/\mathbb{Q}_p).
\]

**Remark 19.** The local reciprocity map is not, as stated, an isomorphism! First note that it couldn’t possibly be a continuous isomorphism, as \( \mathbb{Q}_p^\times \) is not compact while \( \text{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \) is profinite and hence compact. But in fact, not only is \( \phi \) not continuous, it is not surjective. We will see this below after we discuss the Local Kronecker-Weber theorem (Theorem 20).
5. Local Kronecker-Weber Theorem

In this section we will explain how one can easily define the reciprocity map when working over \( \mathbb{Q}_p \). The challenge of local class field theory is to prove that property (2) of Theorem 18 is satisfied by this map.

A finite extension of a field \( K \) is said to be cyclotomic if it is a subfield of an extension \( K(\zeta)/K \) where \( \zeta \) is a root of unity.

**Theorem 20** (Kronecker-Weber). Every abelian extension of \( \mathbb{Q}_p \) is cyclotomic.

We will not prove this theorem. The maximal unramified extension \( \mathbb{Q}_p^{un}/\mathbb{Q}_p \) is obtained by adjoining to \( \mathbb{Q}_p \) all roots of unity of order relatively prime to \( p \). Adjoining \( p \)-power roots of unity to \( \mathbb{Q}_p \) yields ramified abelian extensions. One thus deduces the following:

**Corollary 21.** Let \( \mathbb{Q}_p(\mu_{p^n}) \) denote the infinite extension of \( \mathbb{Q}_p \) obtained by adjoining all \( p \)-power roots of unity to \( \mathbb{Q}_p \). Then
\[
\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\mu_{p^n}) \cdot \mathbb{Q}_p^{un}.
\]

**Remark 22.** It is not true that every finite abelian extension \( L/\mathbb{Q}_p \) is of the form \( L = K_1 K_2 \) where \( K_1/\mathbb{Q}_p \) is totally ramified and \( K_2/\mathbb{Q}_p \) is unramified. See Example 4.13 in Milne’s notes on class field theory for an example.

We can now define the local reciprocity map. First note that, just as over \( \mathbb{Q} \), \( \text{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \), where \( \zeta_{p^n} \) is a primitive \( p^n \)th root of unity. Taking a limit of these compatible isomorphisms yields the following isomorphism:
\[
\text{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \cong \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) \times \text{Gal}(\mathbb{Q}_p^{un}/\mathbb{Q}_p)
\cong \lim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \times \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)
\cong \mathbb{Z}^\times_p \times \hat{\mathbb{Z}}.
\]

In a previous lecture we have seen that \( \mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times p\mathbb{Z} \). In this simple cyclotomic case over \( \mathbb{Q}_p \), the reciprocity map is defined to be the identity on \( \mathbb{Z}^\times_p \), and \( p \) is mapped to \( 1 \in \hat{\mathbb{Z}} \). Recall that \( 1 \in \hat{\mathbb{Z}} \) corresponds to the Frobenius automorphism in \( \text{Gal}(\mathbb{Q}_p^{un}/\mathbb{Q}_p) \cong \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \). It is clear that the reciprocity map is injective but not surjective, although it does have dense image. The reciprocity map satisfies property (1) of Theorem 18 by definition, but it takes real work to establish property (2).

**Example 23.** Let \( U_n = (1 + p^n\mathbb{Z}) \times p\mathbb{Z} \) for each \( n \geq 1 \), which we regard as a subgroup of \( \mathbb{Q}_p^\times \). It is a subgroup of index \( p^{n-1}(p-1) \) for each \( n \geq 1 \), and thus corresponds to a subfield of \( \mathbb{Q}_p^{ab} \). Since the entire factor \( p\mathbb{Z} \) is contained in \( U_n \), the fixed field of \( U_n \) must be invariant under Frobenius, and hence must be a totally ramified extension. An element of the form \( 1 + p^n\alpha \in (1 + p^n\mathbb{Z}) \) acts on \( \mu_{p^n} \) as \( \zeta \mapsto \zeta^{1+p^n\alpha} \). It follows that \( U_n \) corresponds to the extension \( \mathbb{Q}_p(\mu_{p^n}) \) for all \( n \geq 1 \).

**Example 24.** Let \( V_n = \mathbb{Z}_p^\times \times p^n\mathbb{Z} \) for \( n \geq 1 \). Under the local reciprocity map,
\[
(\mathbb{Z}_p^\times \times p^n\mathbb{Z})/V_n \cong \text{Gal}(L_n/\mathbb{Q}_p),
\]
where \( L_n/\mathbb{Q}_p \) denotes the unique unramified extension of \( \mathbb{Q}_p \) of degree \( n \).