• **Classfield Theory** In brief, *global* classfield theory classifies *abelian* extensions of *number fields*, while *local* classfield theory does the analogous things for *local fields*, finite extensions of $\mathbb{Q}_p$.

The details subsume all known (abelian) **reciprocity laws**.

Main Theorem of Global Classfield Theory (classical form): The abelian (Galois) extensions K of a number field k are in bijection with generalized ideal class groups, which are quotients of *ray class groups* of *conductor* (a non-zero ideal) $\mathfrak{f}$

$$I(\mathfrak{f})/P_{\mathfrak{f}}^{+}$$

$$||$$

$$\frac{\text{fractional ideals prime to } \mathfrak{f}}{\text{principal ideals with totally positive generators 1 mod } \mathfrak{f}}$$

Further, the bijection sends a given generalized ideal class group to the (abelian) *Galois group* of the extension, via the *Artin/Frobenius* map/symbols $\mathfrak{p} \to (\mathfrak{p}, K/k)$ [see below].

Main Theorem of Local Classfield Theory: The abelian (Galois) extensions K of a local field k are in bijection with the open, finite-index subgroups of $k^\times$, by

$$K/k \longleftrightarrow k^\times/N_k^K K^\times$$

This bijection is given by an isomorphism of the Galois group with $k^\times/N_k^K K^\times$ via Artin/Frobenius.

Cyclic local-global principle for norms: In a *cyclic* extension K/k of number fields, an element of k is a *global norm* if and only if it is a *local norm everywhere.* That is, for $\alpha \in k$,

$$\alpha \in N_k^K(K^\times) \iff \alpha \in N_{k_v}^{K_w}(K_w^\times) \text{ for all } v, w$$

The most intelligible proof uses *zeta functions of simple algebras.*

To approach classfield theory, it is useful to progress from simple situations to complicated: *finite* fields, *local* fields, *number* fields.

Indeed, the simplest part of the Galois theory of local fields is described by the Galois theory of their residue fields. The same is true of number fields.

As a diagnostic, if we can't understand finite extensions of *finite* fields, most likely we'll not understand finite extensions of *local* fields and *number* fields.

Further, as below, all finite finite-field extensions are generated by *roots of unity*. Thus, extensions of local fields and number fields generated by roots of unity (*cyclotomic* extensions) are the first and canonical examples of abelian extensions. Extensions $k(\sqrt[n]{a})$ for k containing n^{th} roots of unity (*Kummer extensions*) are next.

In fact, over $\mathbb{Q}$ itself, classfield theory is provably the study of cyclotomic extensions (*Kronecker-Weber theorem*).

Finite fields: Recall the classification of finite algebraic field extensions of $\mathbb{F}_p$:

Claim: inside a fixed algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, for each integer n there is a unique field extension K of degree n over $\mathbb{F}_p$. It is the collection of roots of $x^{p^n} - x = 0$ in the fixed algebraic closure.

Proof: On one hand, a finite multiplicative subgroup of a field is *cyclic*, else there'd be too many roots of unity of some order. A field extension of $\mathbb{F}_p$ of degree n is an n-dimensional $\mathbb{F}_p$-vectorspace, so has p^n elements. The non-zero elements form a cyclic group of order $p^n - 1$. These, together with 0, are roots of $x^{p^n} - x = 0$.

On the other hand, inside the algebraic closure there is a splitting field of $x^{p^n} - x$. ///

Remark: The same proof works over arbitrary finite fields.

Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$: is *cyclic*, generated by the Frobenius element $\alpha \to \alpha^p$.

Proof: The Frobenius element stabilizes $\mathbb{F}_{p^n}$, since $\alpha^{p^n} = \alpha$ implies

$$(\alpha^p)^{p^n} = \alpha^{p^{n+1}} = (\alpha^{p^n})^p = \alpha^p$$

On the other hand, the fixed points of the Frobenius in $\mathbb{F}_{p^n}$ are roots of $x^p - x = 0$, giving exactly $\mathbb{F}_p$. Similarly, the action of Frobenius on $\mathbb{F}_{p^n}$ really is of order n. Thus, by Galois theory, the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is *cyclic* order n generated by Frobenius. ///

Remark: The same proof works over arbitrary finite fields.

Surjectivity of norms on finite fields: The Galois norm $N : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is *surjective:*

Proof: The norm is

$$N\alpha \;=\; \alpha \cdot \alpha^p \cdot \ldots \cdot \alpha^{p^{n-1}} \;=\; \alpha^{1+p+p^2+\ldots+p^{n-1}} \;=\; \alpha^{\frac{p^n-1}{p-1}}$$

Note that the exponent divides $p^n - 1$. In a finite cyclic group of order ℓ, for every divisor k of ℓ, the map $g \to g^k$ surjects to the unique subgroup of order ℓ/k. Here, the Galois norm surjects to $\mathbb{F}_p^\times$. ///

Remark: A similar result holds for extensions of arbitrary finite fields.

Surjectivity of traces on finite fields: The Galois trace $\mathrm{tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is *surjective:*

Proof: The trace is

$$\mathrm{tr}\,\alpha \;=\; \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}$$

This is a linear combination (all coefficients 1) of field homomorphisms $\mathbb{F}_{p_n} \to \mathbb{F}_{p^n}$. The desired assertion is a very special case of

Linear independence of characters: Let $\chi_j : k \to \Omega$ be distinct field maps. For $c_j \in \Omega$, $\sum_j c_j \chi_j = 0$ as a map $k \to \Omega$ only for c_j all 0.

Proof: Let $\sum_j c_j \chi_j = 0$ be a shortest non-trivial relation, renumbering as convenient...

Divide through by c_1, so

$$\chi_1 + c_2\chi_2 + \ldots = 0 \qquad \text{(with } c_2 \neq 0\text{)}$$

Let $0 \neq x \in k$ such that $\chi_1(x) \neq \chi_2(x)$. Then

$$0 = \chi_1(xy) + c_2\chi_2(xy) + \ldots = \chi_1(x) \cdot \Big(\chi_1(y) + c_2 \frac{\chi_2(x)}{\chi_1(x)} \chi_2(y) + \ldots\Big)$$

Dividing by $\chi_1(x)$ and subtracting gives a shorter relation, contradiction. ///

The Galois maps of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ are linearly independent, are $\mathbb{F}_p$-linear, so trace is a *not-identically-zero* $\mathbb{F}_p$-linear map $\mathbb{F}_{p^n} \to \mathbb{F}_p$. Since $\mathbb{F}_p$ is one-dimensional over itself, this is surjective. ///

Remark: A similar result holds for extensions of arbitrary finite fields.

Unramified extensions of $\mathbb{Q}_p$: Inside a fixed algebraic closure of $\mathbb{Q}_p$, for each positive integer n there is a unique *unramified* extension k of $\mathbb{Q}_p$ of degree n over $\mathbb{Q}_p$. It is generated by a primitive $p^n - 1$ root of unity.

Proof: Recall that the local ramification degree e and residue class field extension degree f satisfy $ef = n$. The unramified-ness is $e = 1$, so $f = n$. There is a primitive $p^n - 1$ root of unity in $\mathbb{F}_{p^n}$.

Let Φ be the $(p^n - 1)^{th}$ cyclotomic polynomial. It has no repeated roots mod p. We do not claim that Φ is irreducible over $\mathbb{Q}_p$. (It probably isn't.) Let $\zeta_1 \in \mathfrak{o}_k$ reduce to a primitive $p^n - 1$ root mod p, so $\Phi(\zeta_1) = 0$ mod p and $\Phi'(\zeta_1) \neq 0$ mod p. Hensel. ///

Remark: The same proof works over arbitrary local fields.

Frobenius elements in Galois groups over $\mathbb{Q}_p$

In $k/\mathbb{Q}_p$, unramified or ramified, there is certainly a unique prime $\mathfrak{p}$ over p. Thus, the *decomposition group* $G_\mathfrak{p} = \{g \in \mathrm{Gal}(k/\mathbb{Q}_p) : g\mathfrak{p} = \mathfrak{p}\}$ is the whole Galois group $\mathrm{Gal}(k/\mathbb{Q}_p)$. Recall that $G_\mathfrak{p}$ *surjects* to the residue field Galois group, which is cyclic order n, generated by Frobenius.

In general, the kernel of the map of $G_\mathfrak{p}$ to the residue field Galois group is the inertia subgroup. Here, there cannot be a non-trivial kernel, since the residue field extension degree is equal to that of the local field extension degree.

Thus, $\mathrm{Gal}(k/\mathbb{Q}_p) = G_\mathfrak{p}$ is cyclic order n, with canonical generator also called *Frobenius*, characterized by reducing mod p to the finite-field Frobenius.

Remark: The same proof works for unramified extensions of arbitrary local fields.

Norm map in unramified extensions $k/\mathbb{Q}_p$

Claim: The Galois norm $N : k \to \mathbb{Q}_p$ gives a *surjection* $\mathfrak{o}_k^\times \to \mathbb{Z}_p^\times$.

Proof: Surjectivity of finite-field norm and trace, and completeness. Frobenius $\varphi \in \mathrm{Gal}(k/\mathbb{Q}_p)$ satisfies $\varphi(\alpha) = \alpha^p \bmod p\mathfrak{o}$, so, mod $p\mathfrak{o}$

$$N\alpha \;=\; \alpha\,\alpha^p \,\ldots\, \alpha^{p^{n-1}} \;=\; \alpha^{1+p+p^2+\ldots+p^{n-1}} \;=\; \alpha^{\frac{p^n-1}{p-1}} \qquad (\mathrm{mod}\ p\mathfrak{o})$$

This reduces the question to proving surjectivity to $1 + p\mathbb{Z}_p$. By surjectivity of trace on finite fields, $\mathrm{tr}^k_{\mathbb{Q}_p}\,\mathfrak{o}_k \;=\; \mathbb{Z}_p$. Thus, given $1 + p\alpha$ with $\alpha \in \mathbb{Z}_p$, there is $\beta \in \mathfrak{o}$ with $\mathrm{tr}(\beta) = \alpha$. Thus, $N(1 + p\beta) = 1 + p\alpha \bmod p^2$. This reduces the question to proving surjectivity to $1 + p^2\mathbb{Z}_p$. Continuing, using completeness, the sequence of cumulative adjustments converges. ///

Remark: The same proof works for unramified extensions of arbitrary local fields.

A very special sub-case:

Unramified **local classfield theory:**

(Mock) Theorem: The unramified extensions k of $\mathbb{Q}_p$ are in bijection with finite-index subgroups of $\mathbb{Q}_p^\times$ containing $\mathbb{Z}_p^\times$, by

$$\text{finite-index subgroup } H \supset \mathbb{Z}_p^\times \quad \longleftrightarrow \quad N_{\mathbb{Q}_p}^k(k^\times)$$

The Galois group is $\mathrm{Gal}(k/\mathbb{Q}_p) \approx \mathbb{Q}_p^\times / N_{\mathbb{Q}_p}^k(k^\times)$, via the map to Artin/Frobenius:

$$\big(\text{Frobenius } x \to x^p\big) \quad \longleftarrow \quad p$$

Remark: The analogous result holds for all local fields.

Proof: We have shown that an unramified extension k of $\mathbb{Q}_p$ of degree n is cyclic Galois, obtained by adjoining a primitive $(p^n - 1)^{th}$ root of unity ω, and the map from $\mathrm{Gal}(k/\mathbb{Q}_p)$ to the Galois group of residue fields is an isomorphism. Thus, the Frobenius generates $\mathrm{Gal}(k/\mathbb{Q}_p)$, and is order n.

Since the norm $N^k_{\mathbb{Q}_p}$ is surjective $\mathfrak{o}_k^\times \to \mathbb{Z}_p^\times$, $N^k_{\mathbb{Q}_p}(k^\times)$ is *open*. Also, $N^k_{\mathbb{Q}_p}(p) = p^n$. Thus, $\mathbb{Q}_p^\times / N^k_{\mathbb{Q}_p}(k^\times) \approx p^{\mathbb{Z}}/p^{n\mathbb{Z}}$, which gives the Galois group, by the map to Frobenius.

On the other hand, for $H \supset \mathbb{Z}_p^\times$ of finite index n, since $\mathbb{Q}_p^\times/\mathbb{Z}_p^\times \approx p^{\mathbb{Z}}$, necessarily $H = p^{n\mathbb{Z}} \cdot \mathbb{Z}_p^\times$. Adjoining a primitive $(p^n - 1)^{th}$ root of unity produces an unramified degree n extension k such that $N^k_{\mathbb{Q}_p}(k^\times) = H$. ///