- **Classfield Theory...**

- Slightly refined main statements
- Recollection of quadratic example
- Recap Hilbert's theorem 90

- Herbrand quotients: veiled homological ideas
- Recollection of topological antecedents: counting holes
- Toward Hilbert's theorem 90 as cohomology
- Cyclic extensions of local fields

Putting pieces of classfield theory together:

Local classfield theory asserts that the Galois groups of finite abelian extensions K of a local field k are exactly the quotients $k^\times/N_k^K(K^\times) \xrightarrow[\approx]{\alpha_{L/k}} \mathrm{Gal}(K/k)$. The **Artin** or **reciprocity law** maps to Galois groups are *natural*, in the sense that, for finite abelian extensions $L \supset K \supset k$ there is a commutative diagram

$$\begin{array}{ccc} k^\times/N_k^L(L^\times) & \xrightarrow{\alpha_{L/k}} & \mathrm{Gal}(L/k) \\ {\scriptstyle \mathrm{quot}}\downarrow & & \downarrow{\scriptstyle \mathrm{quot}} \\ k^\times/N_k^K(K^\times) & \xrightarrow[\alpha_{K/k}]{} & \mathrm{Gal}(K/k) \end{array}$$

For an abelian extension of number fields K/k, the *global* Artin/reciprocity map $\alpha_{K/k} : \mathbb{J} \to \mathrm{Gal}(K/k)$ is *essentially the product of the local ones...*

Recall: For $\mathfrak{p}$ in $\mathfrak{o}_k$ and $\mathfrak{P}|\mathfrak{p}$ in $\mathfrak{o}_K$ unramified in abelian K/k, the inertia subgroup of the decomposition group $G_\mathfrak{p} \subset \mathrm{Gal}(K/k)$ is trivial, $G_\mathfrak{p}$ is generated by the Artin element $(\mathfrak{p}, K/k)$.

The corresponding unramified extension of completions K_w/k_v is *cyclic* with Galois group generated by the local Artin element $(\mathfrak{m}_v, K_w/k_v)$ with $\mathfrak{m}_v$ the unique non-zero prime in $\mathfrak{o}_v$. The local Artin/reciprocity map $\alpha_{w/v} : k_v^\times \to \mathrm{Gal}(K_w/k_v)$ is

$$\alpha_{w/v}(x) \;=\; (\mathfrak{m}_v, K_w/k_v)^{\mathrm{ord}_v x} \qquad\qquad (\text{unramified } K_w/k_v)$$

Identifying the two cyclic groups $\mathrm{Gal}(K_w/k_v) \approx G_\mathfrak{p}$ by identifying their corresponding Artin elements $(\mathfrak{m}_v, K_w/k_v) \longleftrightarrow (\mathfrak{p}, K/k)$, we can consider the local Artin map as mapping to $G_\mathfrak{p}$, and

$$\alpha_{w/v} \;:\; k_v^\times \;\longrightarrow\; \mathrm{Gal}(K_w/k_v) \;\approx\; G_\mathfrak{p} \;\subset\; \mathrm{Gal}(K/k)$$

With the identification $\text{Gal}(K_w/k_v) \approx G_{\mathfrak{p}} \subset \text{Gal}(K/k)$ at unramified places, define the *global* Artin/reciprocity map $\alpha_{K/k} : \mathbb{J} \longrightarrow \text{Gal}(K/k)$ by

$$\alpha_{K/k}(x) = \prod_v \prod_{w|v} \alpha_{w/v}(x_v) \qquad\qquad (\text{for } x = \{x_v\} \in \mathbb{J}_k)$$

Remark: For the moment, we seem not to know how to define local Artin/reciprocity maps at *ramified* primes.

Remark: Local norms at unramified K_w/k_v are *surjective* to local units, so the product is *finite*.

The *critical* part of the assertion of global classfield theory is that the global $\alpha_{K/k}$ *factors through* the idele class group $\mathbb{J}_k/k^\times$.

It is a *local* fact that $\alpha_{w/v} : k_v^\times \to \text{Gal}(K_w/k_v)$ factors through $k_v^\times/N_{k_v}^{K_w} K_w^\times$ and gives an *isomorphism* $\alpha_{w/v} : k_v^\times/N_{k_v}^{K_w} K_w^\times \to \text{Gal}(K_w/k_v)$. Thus, $\alpha_{K/k}$ factors similarly.

And $\alpha_{K/k} : \mathbb{J}_k/k^\times N_k^K \mathbb{J}_K \longrightarrow \text{Gal}(K/k)$ is an *isomorphism*.

Significance of factoring through $\mathbb{J}/k^\times$ and $\mathbb{J}/k^\times N_k^K \mathbb{J}_K$

Since norms in unramified extensions of non-archimedean fields are *surjective* to local units, and norms on archimedean fields are open maps, the image $N_k^K \mathbb{J}_K$ is *open* in $\mathbb{J}_k$. Thus, the local and global Artin maps are *continuous*.

The latter open-ness/continuity reformulates *part* of the classical assertion that the Artin map **has a conductor**. But the difficult part is proving $k^\times$-invariance.

By Fujisaki's Lemma, since the product of norms at archimedean places includes *the ray* $\{(t^{1/N}, \ldots, t^{1/N}, 1, 1, \ldots) : t > 0\}$ with $N = r_1 + r_2$, the quotient $\mathbb{J}_k/k^\times N_k^K \mathbb{J}_K$ is *finite*, in any case.

Recall how the fact that the quadratic *norm residue* symbol factors through $\mathbb{J}_k/k^\times$ proves reciprocity for the quadratic Hilbert symbol, and then more classical forms of quadratic reciprocity...

For global field k with *completions* k_v of k, for K a *quadratic* extension of k, put

$$K_v = K \otimes_k k_v$$

The **local norm residue symbol** $\nu_v : k_v^\times \to \{\pm 1\}$ is

$$\nu_v(\alpha) = \begin{cases} +1 & (\text{for } \alpha \in N(K_v^\times)) \\ \\ -1 & (\text{for } \alpha \notin N(K_v^\times)) \end{cases}$$

For $k_v = \mathbb{Q}_p$ with odd p, we have proven the small *local*
Theorem:

$$[k_v^\times : N(K_v^\times)] = \begin{cases} 2 & (\text{when } K_v \text{ is a field}) \\ \\ 1 & (\text{when } K_v \approx k_v \times k_v) \end{cases}$$

Cor: ν_v is a group homomorphism $k_v^\times \to \{\pm 1\}$. ///

We grant ourselves... **Theorem:** the quadratic norm-residue map ν is $k^\times$-invariant: it *factors through* $\mathbb{J}/k^\times$.

This is a *reciprocity law*, and we saw earlier that this entails more classical-looking reciprocity laws. We recall the connections:

Quadratic Hilbert symbols For $a, b \in k_v$ the (quadratic) Hilbert symbol is

$$(a,b)_v = \begin{cases} 1 & (\text{if } ax^2 + by^2 = z^2 \text{ has non-trivial solution in } k_v) \\ \\ -1 & (\text{otherwise}) \end{cases}$$

Corollary: For $a, b \in k^\times$, we have $\Pi_v \ (a,b)_v = 1$.

Proof: For b a non-square in $k^\times$, $(a,b)_v$ is $\nu_v(a)$ for the field extension $k(\sqrt{b})$, and reciprocity for the norm residue symbol gives the result for the Hilbert symbol. ///

Traditional-looking quadratic reciprocity laws follow from that reciprocity for the quadratic Hilbert symbol. Define

$$\left(\frac{x}{v}\right)_2 = \begin{cases} 1 & (\text{for } x \text{ a non-zero square mod } v) \\ 0 & (\text{for } x = 0 \text{ mod } v) \\ -1 & (\text{for } x \text{ a non-square mod } v) \end{cases}$$

Quadratic Reciprocity ('main part'): For π and ϖ two elements of $\mathfrak{o}$ generating distinct odd prime ideals,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 = \Pi_v \, (\pi, \varpi)_v$$

where v runs over all *even or infinite* primes, and $(,)_v$ is the (quadratic) Hilbert symbol.

Proof: Claim that, since $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$ are odd primes,

$$(\pi, \varpi)_v \;=\; \begin{cases} \left(\frac{\varpi}{\pi}\right)_2 & \text{for } v = \pi\mathfrak{o} \\ \left(\frac{\pi}{\varpi}\right)_2 & \text{for } v = \varpi\mathfrak{o} \\ 1 & \text{for } v \text{ odd and } v \neq \pi\mathfrak{o}, \varpi\mathfrak{o} \end{cases}$$

Let $v = \pi\mathfrak{o}$. Suppose that there is a solution x, y, z in k_v to

$$\pi x^2 + \varpi y^2 \;=\; z^2$$

Via the ultrametric property, $\mathrm{ord}_v y$ and $\mathrm{ord}_v z$ are identical, and less than $\mathrm{ord}_v x$, since ϖ is a v-unit and $\mathrm{ord}_v \pi x^2$ is *odd*. Multiply through by π^{2n} so that $\pi^n y$ and $\pi^n z$ are v-units. Then ϖ must be a square modulo v.

On the other hand, when ϖ is a square modulo v, use Hensel's lemma to infer that ϖ is a square in k_v. Then

$$\varpi y^2 \;=\; z^2$$

certainly has a non-trivial solution.

For v an odd prime distinct from $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$, π and ϖ are v-units. When ϖ is a square in k_v, $\varpi \;=\; z^2$ has a solution, so the Hilbert symbol is 1. For unit ϖ not a square in k_v, the quadratic field extension $k_v(\sqrt{\varpi})$ has the property that the norm map is *surjective* to units in k_v. Thus, there are $y, z \in k_v$ so that

$$\pi \;=\; N(z + y\sqrt{\varpi}) \;=\; z^2 - \varpi y^2$$

Thus, all but even-prime and infinite-prime quadratic Hilbert symbols are quadratic symbols. ///

Simplest example: For two (positive) odd prime numbers p, q, we prove that Gauss' quadratic reciprocity

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (-1)^{(p-1)(q-1)/4}$$

From quadratic Hilbert reciprocity,

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (p,q)_2 (p,q)_\infty$$

Indeed, since both p, q are positive, the equation

$$px^2 + qy^2 = z^2$$

has non-trivial *real* solutions x, y, z. That is, the $\mathbb{Q}_\infty$ Hilbert symbol $(p,q)_\infty$ is 1.

Therefore, only the 2-adic Hilbert symbol contributes to the right-hand side of Gauss' formula:

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (p,q)_2$$

Hensel's lemma shows that the solvability of this equation, for p, q both 2-adic units, depends only upon their residue classes mod 8.

The usual formula $(-1)^{(p-1)(q-1)/4}$ is just one way of interpolating the 2-adic Hilbert symbol by elementary-looking formulas. ///

Remark: Anticipating that general classfield theory is couched in terms of *norms*, we should expect analogous recovery of other reciprocity laws.

Recap:

Hilbert's Theorem 90: In a field extension K/k of degree n with cyclic Galois group generated by σ, the elements in K of norm 1 are exactly those of the form $\sigma\alpha/\alpha$ for $\alpha \in K$. ///

Hilbert's Theorem 90 gives another (the usual?) proof of

Corollary: A cyclic degree n extension K/k of k containing n^{th} roots of unity and characteristic not dividing n is obtained by adjoining an n^{th} root. ///

Additive version of Theorem 90: Let K/k be cyclic of degree n with Galois group generated by σ. Then $\mathrm{tr}_k^K(\beta) = 0$ if and only if there is $\alpha \in K$ such that $\beta = \alpha - \alpha^\sigma$.

Corollary: *(Artin-Schreier extensions)* Let K/k be cyclic of order p in characteristic p. Then there is $K = k(\alpha)$ with α satisfying an (Artin-Schreier) equation $x^p - x + a = 0$ with $a \in k$. ///

Post-1940's reformulations: Chevalley 1940, Weil 1951, Hochschild-Nakayama 1952, ... To ground this, recast some things we already know, such as *Hilbert's Theorem 90,* in other terms.

Herbrand quotients: veiled homological ideas

Homological algebra includes computational devices extending linear algebra and counting procedures. Motivations also come from (algebraic) topology, defining and counting *holes*.

It is easy enough to *define* the **Herbrand quotient**, although explaining its significance, and the meaning of the Key Lemma, requires more effort:

Let A be an abelian group, with maps $f : A \to A$ and $g : A \to A$, such that $f \circ g = 0$ and $g \circ f = 0$.

$$q(A) \;=\; q_{f,g}(A) \;=\; \text{Herbrand quotient of } A, f, g \;=\; \frac{[\ker f : \operatorname{im} g]}{[\ker g : \operatorname{im} f]}$$

Inscrutable Key Lemma: For finite A, $q(A) \;=\; 1$. For f-stable, g-stable subgroup $A \subset B$ with $f, g : B \to B$, we have $q(B) = q(A) \cdot q(B/A)$, in the usual sense that if two are finite, so is the third, and the relation holds.

The *keywords* are that this Lemma is about *Euler-Poincaré characteristics* of the short exact sequence of *complexes*

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow f & & \downarrow f & & \downarrow f & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & B/A & \longrightarrow & 0 \\
 & & \downarrow g & & \downarrow g & & \downarrow g & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & B/A & \longrightarrow & 0 \\
 & & \downarrow f & & \downarrow f & & \downarrow f & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & B/A & \longrightarrow & 0 \\
 & & \downarrow g & & \downarrow g & & \downarrow g & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

What does this mean?

First, quick definitions stripped of origins, motivation, or purpose: A *complex* of abelian groups A_i is a family of homomorphisms

$$\cdots \longrightarrow A_i \xrightarrow{f_i} A_{i-1} \xrightarrow{f_{i-1}} \cdots$$

with the *composition of any two consecutive maps* 0, that is, with $f_{i-1} \circ f_i = 0$, for all i. The **(co)homology**, with superscript or subscript depending on context and numbering conventions, is

$$H_i(\text{the complex}) \;=\; H^i(\text{the complex}) \;=\; \frac{\ker f_i}{\operatorname{im} f_{i\pm 1}}$$

The utility of this requires explanation. Indeed, the history of the interaction of linear algebra and algebraic topology (as *counting holes*) is tangled.