- **Classfield Theory...**

- Slightly refined main statements
- Interlude: finiteneness of ramification
- 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: 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:*

At unramified K_w/k_v, the local Artin/reciprocity map $k_v^\times \to \mathrm{Gal}(K_w/k_v)$ is $\alpha_{w/v}(x) = (\mathfrak{m}_v, K_w/k_v)^{\mathrm{ord}_v x}$. Identifying the two cyclic groups $\mathrm{Gal}(K_w/k_v) \approx G_\mathfrak{p}$ by identifying their corresponding Artin elements $(\mathfrak{m}_v, K_w/k_v) \longleftrightarrow (\mathfrak{p}, K/k)$, consider the local Artin map as mapping to $G_\mathfrak{p}$, and

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

Then the *global* Artin/reciprocity map $\alpha_{K/k} : \mathbb{J} \longrightarrow \mathrm{Gal}(K/k)$ is

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

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

Interlude: finiteness of ramification

It is important that only finitely-many primes *ramify* in $\mathfrak{o}_K/\mathfrak{o}_k$, where K/k is a finite extension of number fields.

In fact, finiteness of ramification is a more general algebraic fact:

Theorem: *Only finitely many primes ramify* in the integral closure $\mathfrak{O}$ of a Dedekind domain $\mathfrak{o}$ in a finite separable extension K/k of the field of fractions k of $\mathfrak{o}$.

The proof requires some preparation. The *inverse different* $\mathfrak{d}^{-1}_{\mathfrak{O}/\mathfrak{o}}$ of $\mathfrak{O}/\mathfrak{o}$ is

$$\mathfrak{d}^{-1}_{\mathfrak{O}/\mathfrak{o}} \;=\; \{x \in K \;:\; \mathrm{tr}_k^K(x\mathfrak{O}) \subset \mathfrak{o}\}$$

Proposition: The inverse different is a fractional ideal of $\mathfrak{O}$ containing $\mathfrak{O}$.

Proof: Since $\mathrm{tr}_k^K(\mathfrak{O}) \subset \mathfrak{o}$, certainly $\mathfrak{O} \subset \mathfrak{d}_{K/k}^{-1}$.

Given a k-basis x_i of K, we can adjust by a non-zero constant in k so that all x_i are in $\mathfrak{O}$. Let $\widehat{x}_i$ be the dual basis with respect to the trace pairing, which by separability is non-degenerate.

Since $\sum_i \mathfrak{o}x_i \subset \mathfrak{O}$, certainly $\mathfrak{d}^{-1} \subset \sum_i \mathfrak{o}\widehat{x}_i$, a finitely-generated $\mathfrak{o}$-module inside K. Since $\mathfrak{o}$ is *Noetherian*, every submodule of a finitely-generated $\mathfrak{o}$-module is finitely-generated, so $\mathfrak{d}^{-1}$ is finitely-generated as an $\mathfrak{o}$-module. Thus, it is certainly finitely-generated as an $\mathfrak{O}$-module, so is a fractional ideal. Since $\mathfrak{d}^{-1} \supset \mathfrak{O}$, its inverse is contained in $\mathfrak{O}$. ///

Given the proposition, it makes sense to define the *different* $\mathfrak{d}_{\mathfrak{O}/\mathfrak{o}}$ to be the fractional-ideal inverse of $\mathfrak{d}^{-1}_{\mathfrak{O}/\mathfrak{o}}$. When the Dedekind rings $\mathfrak{o} \subset k$ and $\mathfrak{O} \subset K$ are understood, we may write

$$\mathfrak{d}_{K/k} \;=\; \mathfrak{d}_{\mathfrak{O}/\mathfrak{o}}$$

Proposition: The different is *multiplicative in towers*, that is, for finite separable extensions $k \subset K \subset L$, with k the field of fractions of Dedekind $\mathfrak{o}_k$, and for integral closures $\mathfrak{o}_K$ and $\mathfrak{o}_L$ of $\mathfrak{o}_k$ in K and L,

$$\mathfrak{d}_{L/k} \;=\; \mathfrak{d}_{L/K} \cdot \mathfrak{d}_{K/k}$$

Proof: On one hand, with $x \in L$ and $y \in K$ and $\mathrm{tr}^L_K(x\mathfrak{o}_L) \subset \mathfrak{o}_K$ and $\mathrm{tr}^K_k(y\mathfrak{o}_K) \subset \mathfrak{o}_k$, certainly

$$\mathrm{tr}^L_k(xy\mathfrak{o}_L) = \mathrm{tr}^K_k \mathrm{tr}^L_K(xy\mathfrak{o}_L) = \mathrm{tr}^K_k(y \cdot \mathrm{tr}^L_K(x\mathfrak{o}_L)) \subset \mathrm{tr}^K_k(y\mathfrak{o}_K) \subset \mathfrak{o}_k$$

gives $\mathfrak{d}^{-1}_{L/K} \cdot \mathfrak{d}^{-1}_{K/k} \subset \mathfrak{d}^{-1}_{L/k}$. Conversely, ...

for $x \in \mathfrak{d}_{L/k}^{-1}$,

$$\mathrm{tr}_k^K(\mathrm{tr}_K^L x\mathfrak{o}_L \cdot \mathfrak{o}_K) \;=\; \mathrm{tr}_k^K(\mathrm{tr}_K^L x\mathfrak{o}_L) \;=\; \mathrm{tr}_k^L(x\mathfrak{o}_L) \;\subset\; \mathfrak{o}_k$$

Thus, $\mathrm{tr}_K^L(\mathfrak{d}_{L/K}^{-1}) \subset \mathfrak{d}_{K/k}^{-1}$, and for $x \in \mathfrak{d}_{L/k}^{-1}$

$$\mathrm{tr}_K^L(\mathfrak{d}_{K/k} \cdot x\mathfrak{o}_L) \;=\; \mathfrak{d}_{K/k} \cdot \mathrm{tr}_K^L(x\mathfrak{o}_L) \;\subset\; \mathfrak{d}_{K/k} \cdot \mathfrak{d}_{K/k}^{-1} \;=\; \mathfrak{o}_K$$

That is, $\mathfrak{d}_{K/k} \cdot \mathfrak{d}_{L/k}^{-1} \subset \mathfrak{d}_{L/K}^{-1}$. Even though $\mathfrak{d}_{K/k}$ is not a fractional ideal in L, the product $\mathfrak{d}_{K/k} \cdot \mathfrak{d}_{L/k}^{-1}$ is contained in the finitely-generated $\mathfrak{o}_L$-module $\mathfrak{d}_{L/K}^{-1}$, and $\mathfrak{o}_L$ is Noetherian. Thus, that product is a fractional ideal in L. Multiplying the containment through by the ideal $\mathfrak{d}_{L/k} \cdot \mathfrak{d}_{L/K}$ gives $\mathfrak{d}_{K/k} \cdot \mathfrak{d}_{L/K} \subset \mathfrak{d}_{L/k}$. ///

Corollary: There are only finitely-many primes $\mathfrak{p}$ in $\mathfrak{o}_k$ ramifying in $\mathfrak{o}_K/\mathfrak{o}_k$ for finite separable K/k.

Proof: A prime that ramifies in K/k certainly ramifies in the further (finite, separable) extension to the Galois closure of K over k, so it suffices to consider the finite Galois case.

Let $\mathfrak{p} \cdot \mathfrak{o}_K = (\mathfrak{P}_1 \ldots \mathfrak{P}_n)^e$.

$$\mathrm{tr}_k^K(\mathfrak{P}_1^{1-e} \cdot \mathfrak{o}_K) \;=\; \mathfrak{p}^{-1}\mathfrak{p} \cdot \mathrm{tr}_k^K(\mathfrak{P}_1^{1-e}) \;=\; \mathfrak{p}^{-1}\mathrm{tr}_k^K(\mathfrak{p}\mathfrak{P}_1^{1-e})$$

$$\subset\; \mathfrak{p}^{-1}\mathrm{tr}_k^K(\mathfrak{P}_1\mathfrak{P}_2^e \ldots \mathfrak{P}_n^e) \;\subset\; \mathfrak{p}^{-1}\mathrm{tr}_k^K(\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_n)$$

$$\subset\; \mathfrak{p}^{-1} \cdot (\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_n \cap \mathfrak{o}_k) \;\subset\; \mathfrak{p}^{-1} \cdot \mathfrak{p} \;=\; \mathfrak{o}_k$$

Thus, $\mathfrak{P}_1^{1-e} \;\subset\; \mathfrak{d}_{K/k}^{-1}$, which is equivalent to $\mathfrak{d}_{K/k} \;\subset\; \mathfrak{P}_1^{e-1}$, so $\mathfrak{P}_1^{e-1}|\mathfrak{d}_{K/k}$. Since $\mathfrak{d}_{K/k}$ is a non-zero ideal, only finitely-many primes divide it. ///

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: ... 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*

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

What does this mean?

The best-known *Euler characteristic* refers to the numbers of vertices V, edges E, and F faces of a polyhedron, and *Euler's theorem* is that, for *convex* polyhedra,

$$V - E + F \;=\; 2 \qquad\qquad \text{(Euler char of convex polyhedron)}$$

We are concerned with the *linear algebra* in this.

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

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

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.

Recollection of topological antecedents: *counting holes.*

An n-dimensional triangle is an n-*simplex.* A *simplicial complex* [different use of the word!] X is a topological space made by sticking together simplices *in a reasonable way.*

An *orientation* of a simplex is an ordering of its vertices: an oriented n-simplex is a list $\sigma = [v_o, v_1, \ldots, v_n]$ of $n+1$ vertices v_j, with ordering specified modulo even permutations.

The *boundary* $\partial\sigma$ is an alternating sum, in the free group generated by the simplices in X:

$$\begin{aligned}\partial\sigma &= [v_1, \ldots, v_n] - [v_o, v_2, \ldots, v_n] + ... + (-1)^n [v_o, v_1, \ldots, v_{n-1}] \\ &= \sum_{j=0}^{n} (-1)^j [v_o, \ldots, \widehat{v_j}, \ldots, v_n] \qquad \text{(hat denoting omission)}\end{aligned}$$

Permuting the vertices in a simplex multiplies it by the sign of the permutation:

$$[v_{\pi(0)}, v_{\pi(1)}, \ldots, v_{\pi(n)}] = \mathrm{sign}(\pi) \cdot [v_0, v_1, \ldots, v_n]$$

These symbol-pattern occurs in many places...

The abelian group C_n of *n-chains* in X is the free group on oriented n-dimensional simplices in X, and $\partial = \partial_n$ maps $C_n \to C_{n-1}$. A little work shows that $\partial_{n-1} \circ \partial_n = 0$ as a map $C_n \to C_{n-2}$, so we have a *chain complex*

$$\cdots \longrightarrow C_i \xrightarrow{\partial_i} C_{i-1} \xrightarrow{\partial_{i-1}} \cdots \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0$$

with *homology*

$$H_i(X) \;=\; \frac{\ker \partial_i}{\mathrm{im}\, \partial_{i+1}} \;=\; \frac{i\text{-dimensional } \textit{cycles}}{i\text{-dimensional } \textit{boundaries}}$$

It is not obvious, but *the rank of the free part of $H_i(X)$ is the number of i-dimensional holes in X*, in the following sense.

Basic theorem: The n-sphere S^n has $H_i(S^n) = 0$ for $0 < i \neq n$, and $H_n(S^n) = \mathbb{Z}$.

Example computation: First, check that $\partial_1\partial_2 = 0$:

$$\begin{aligned}\partial_1\partial_2[v_0,v_1,v_2] \;&=\; \partial_1\Big([v_1,v_2]-[v_0,v_2]+[v_0,v_1]\Big)\\ &=\; \big([v_2]-[v_1]\big)-\big([v_2]-[v_0]\big)+\big([v_1]-[v_0]\big) \;=\; 0\end{aligned}$$

Second: make a circle S^1 as a hollow triangle X by sticking together three line segments $[v_0,v_1],[v_1,v_2],[v_2,v_0]$. The whole chain complex is not very big:

$$0 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0$$

with C_1 free of rank 3 made from the three line segments $[v_i,v_j]$, and C_0 of rank 3, made from the three vertices.

$$H_1(X) \;=\; \frac{\ker\partial_1}{\operatorname{im}\partial_2} \;=\; \ker\partial_1 \;=\; \mathbb{Z}\cdot\Big([v_0,v_1]+[v_1,v_2]+[v_2,v_0]\Big)$$

Thus, $H_1(X)$ is free, rank one, so this computes that *there is one one-dimensional hole in a circle.*

Another example computation: We can make a 2-sphere by sticking together four oriented triangles along their edges, forming a hollow tetrahedron X: $[v_0, v_1, v_2]$, $[v_1, v_2, v_3]$, $[v_2, v_3, v_0]$, and $[v_3, v_0, v_1]$. The whole chain complex is not very big:

$$0 \longrightarrow C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0$$

with C_2 free of rank 4 made from the four triangles, C_1 of rank 6 made from the six line segments $[v_i, v_j]$, and C_0 of rank 4, made from the four vertices. Note the patterns $\partial_1[v_a, v_b] = [v_a] - [v_b]$ and

$$\partial_2[v_a, v_b, v_c] = [v_b, v_c] - [v_a, v_c] + [v_a, v_b]$$

Linear algebra gives $H_1(X) \approx \{0\}$ and $H_2(X) \approx \mathbb{Z}$, confirming that there is *no* one-dimensional hole in a 2-sphere, but there is a *two-dimensional* hole.

A better computational device: long exact sequence, Mayer-Vietoris, etc

The homology of spheres S^n is best determined *not* by *direct* computation. Under mild hypotheses on topological spaces X, Y, there is a *long exact sequence* (Recall: $A \to B \to C$ is *exact* when $\mathrm{im}\,(A \to B) = \ker(B \to C)$...)

$$\begin{tikzcd}
 & & \dots \arrow[dll] \\
\dots H_i(X \cap Y) \arrow[r] & H_i(X) \oplus H_i(Y) \arrow[r] & H_i(X \cup Y) \arrow[dll] \\
H_{i-1}(X \cap Y) \arrow[r] & H_{i-1}(X) \oplus H_{i-1}(Y) \arrow[r] & H_{i-1}(X \cup Y) \arrow[dll] \\
\dots & &
\end{tikzcd}$$

The long exact sequence is the basic computational device! Compute homology of spheres *by induction...*