- **Classfield Theory...**

- Interlude: finiteness of ramification and the *different* [sic]

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

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.

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 *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 $\mathfrak{O}$. ///

Proposition: The different is *multiplicative in towers*: for finite separable $k \subset K \subset L$, 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

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

Corollary: In finite *Galois* K/k, if $\mathfrak{P}^e|\mathfrak{p}$ then $\mathfrak{P}^{e-1}|\mathfrak{d}_{\mathfrak{O}/\mathfrak{o}}$. ///

Post-1940's reformulations: To warm up, recast some things we already know, such as *Hilbert's Theorem 90.*

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 to *define* the **Herbrand quotient**, although explaining its significance, and the meaning of the Key Lemma, requires more effort: For an abelian group A with maps $f : A \to A$ and $g : A \to A$, with $f \circ g = 0$ 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?

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,

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

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 (with the $\pm$ in the numbering depending on context)

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

with the *composition of any two consecutive maps* $=0$, that is, with $f_{i\pm 1} \circ f_i = 0$, 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:

$$\partial\sigma = [v_1, \ldots, v_n] - [v_o, v_2, \ldots, v_n] + ... + (-1)^n [v_o, v_1, \ldots, v_{n-1}]$$

$$= \sum_{j=0}^{n} (-1)^j [v_o, \ldots, \widehat{v_j}, \ldots, v_n] \qquad \text{(hat denoting omission)}$$

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

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

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*

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

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 sense of the following theorem. Or, perhaps the theorem vindicates *defining* holes in terms of (co-) homology...

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

Basic 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 $\mathrm{im}\,(A \to B) = \ker(B \to C)$...)

$$\begin{array}{ccccc} & & & & \ldots \\ & \swarrow & & & \\ \ldots H_i(X \cap Y) & \longrightarrow & H_i(X) \oplus H_i(Y) & \longrightarrow & H_i(X \cup Y) \\ & \swarrow & & & \\ H_{i-1}(X \cap Y) & \longrightarrow & H_{i-1}(X) \oplus H_{i-1}(Y) & \longrightarrow & H_{i-1}(X \cup Y) \\ & \swarrow & & & \\ \ldots & & & & \end{array}$$

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

Suppose $H_i(S^{n-1}) = 0$ for $0 < i < n-1$ and $H_{n-1}(S^{n-1}) = \mathbb{Z}$. Also, $H_0(S^{n-1}) = \mathbb{Z}$, equivalent to *connectedness*.

S^n is the union of upper hemi-sphere X and lower hemi-sphere Y, with intersection the equator S^{n-1}, setting up the induction.

We grant ourselves that X, Y have no holes, in the sense that their only non-vanishing homology is $H_0(X) = H_0(Y) = \mathbb{Z}$.

Thus, all the higher $H_i(X) \oplus H_i(Y)$'s are 0, and the long exact sequence becomes

$$\begin{array}{ccccc} & & & & \ldots \\ & & & \swarrow & \\ \ldots H_i(S^{n-1}) & \longrightarrow & 0 & \longrightarrow & H_i(S^n) \\ & & & \swarrow & \\ H_{i-1}(S^{n-1}) & \longrightarrow & 0 & \longrightarrow & H_{i-1}(S^n) \\ & & & \swarrow & \\ \ldots & & & & \end{array}$$

That is, the long exact sequence in homology breaks up into smaller exact sequences

$$0 \longrightarrow H_i(S^n) \longrightarrow H_{i-1}(S^{n-1}) \longrightarrow 0 \qquad \text{(for } i > 1\text{)}$$

and, more fussily,

$$0 \to H_1(S^n) \to H_0(S^{n-1}) \to H_0(X) \oplus H_0(Y) \to H_0(S^n) \to 0$$

The *dimension-shifting* conclusion is $H_i(S^n) \approx H_{i-1}(S^{n-1})$, clear for $i > 1$.

For the fussy case $i = 1$, $0 \to H_1(S^n) \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \to 0$ gives $H_1(S^n) = 0$. ///

Remark: This computation is an archetype.

Toward Hilbert's Theorem 90 as cohomology: *The linear algebra that counts holes is useful for counting other things.*

To introduce cohomology as saying useful things about familiar objects, rewrite Hilbert's theorem 90: for $G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$ *cyclic*, letting $t = \sum_{g\in G} g \in \mathbb{Z}[G]$, the additive version of the theorem asserts

$$\frac{\ker t|_K}{\mathrm{im}\,(\sigma-1)|_K} = 0$$

Of course, the multiplicative version *has the same form*, once we realize that for $\beta \in K^\times$, $(\sigma-1)\beta = \sigma\beta/\beta$ and $t\cdot\beta = N_k^K(\beta)$.

An assertion ker/im $= 0$ is of the desired homological form.

Homological algebra puts such quotients into a larger context.

The Artin/reciprocity map will have a natural homological sense.

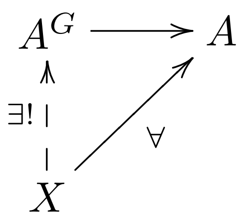
The numerators in Hilbert's Theorem 90 are the kernels of the norm $N_k^K : K^\times \to k^\times$ and trace $\mathrm{tr}_k^K : K \to k$.

$k^\times = (K^\times)^G$ and $k = K^G$ are the G-fixed submodules of $K^\times$ and K, by Galois theory.

Recall that, for a group G and $\mathbb{Z}$-module A with G acting, the *fixed* sub-module A^G is

$$A^G \;=\; \{a \in A \;:\; ga = a \,\text{for all}\, g \in G\}$$

This is the trivial-representation *isotype* in A. This is *characterized* as the *subobject* through which all G-maps from trivial G-modules N to A factor:



(G acting trivially on X)

The denominators in Theorem 90 are explained as follows.

The *co-fixed* quotient module A_G of a G-module A is characterized as the *quotient* through which all G-maps from A to trivial G-modules X factor:

$$\begin{array}{ccc} A_G & \longleftarrow & A \\ {\scriptstyle \exists!}\downarrow & \swarrow{\scriptstyle \forall} & \\ X & & \end{array} \qquad (G \text{ acting trivially on } X)$$

This is A's trivial-representation *co-isotype.* It is provably *constructed* as

$$A_G \;=\; \frac{A}{I_G \cdot A}$$

where I_G is the *augmentation ideal*, the kernel of the *augmentation map* $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$, defined by $\varepsilon g = 1$ for all $g \in G$. Therefore,

$$I_G \;=\; \text{ideal generated in } \mathbb{Z}[G] \text{ by } g - 1 \text{ for } g \in G$$

$I_G \cdot A$ appears in Hilbert's theorem 90 for cyclic G.

For *cyclic* $G = \langle\sigma\rangle$ of order n, with $t = \sum_{g\in G} g$

$$(\sigma - 1)\cdot t \;=\; t\cdot(\sigma-1) \;=\; (\sigma-1)\cdot(1+\sigma+\sigma^2+\ldots+\sigma^{n-1})$$

$$=\; \sigma^n - 1 \;=\; 0 \qquad\qquad (\text{in } \mathbb{Z}[G])$$

Thus, since the composite of any two successive maps is 0, by definition we have a two-sided *complex* fitting the hypotheses of the *Herbrand quotient* situation:

$$\ldots \xrightarrow{t} A \xrightarrow{\sigma-1} A \xrightarrow{t} A \xrightarrow{\sigma-1} A \xrightarrow{t} \ldots$$

(Co-)homology quotients abstracting Theorem 90 are

$$\frac{\ker t|_A}{\mathrm{im}\,(\sigma-1)|_A} \qquad\qquad \frac{\ker(\sigma-1)|_A}{\mathrm{im}\,t|_A}$$