- **Classfield Theory...**

- Herbrand quotients: veiled homological ideas
- Recollection of topological antecedents: counting holes
- Herbrand quotient as Euler-Poincaré characteristic
- Toward Hilbert's theorem 90 as cohomology *cont'd*
- Cyclic extensions of local fields

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*.

Recap the definition of the **Herbrand quotient**, despite its opacity: 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.

More 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)

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

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. In any case, the Herbrand quotient situation involves a *periodic* complex

$$\cdots \longrightarrow A \xrightarrow{f} A \xrightarrow{g} A \xrightarrow{g} A \xrightarrow{f} \cdots$$

and the Herbrand quotient is a ratio of orders of (co-)homology groups.

Basic computational device: long exact sequence

We noted that the homology of spheres S^n is best computed *not* by expressing the spheres as simplicial complexes and using the definition, but by a *long exact sequence* in homology, obtained from the Mayer-Vietoris theorem.

That is, express S^n as the union of two hemispheres, each having trivial homology (no holes!), intersecting at the equator, isomorphic to S^{n-1}.

In this example, the (Mayer-Vietoris) long exact sequence has many 0's, giving $H^i(S^n) \approx H^{i-1}(S^{n-1})$ for $2 \leq i < n$.

Induction on the dimension n of S^n essentially reduces to some low-dimensional and *edge* cases.

These edge cases are nicely explained via *Euler-Poincaré characteristics*, in an algebraic sense, rather than the naive geometric sense $V - E + F$.

Euler-Poincaré characteristics: The fussy edge cases in using the long exact sequence from Mayer-Vietoris to compute homology of spheres are

$$0 \to H_1(S^n) \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \to 0$$

and, at the bottom of the induction,

$$0 \to H_1(S^1) \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \to 0$$

In both cases, the unknown object injects to a free $\mathbb{Z}$-module, so is free. Then the question is obviously its *rank*.

Claim *(about Euler characteristic)***:** In an exact sequence

$$0 \longrightarrow F_1 \longrightarrow F_2 \longrightarrow \ldots \longrightarrow F_{n-1} \longrightarrow F_n \longrightarrow 0$$

of *free* modules F_i, we have $\sum_i (-1)^i \cdot \mathrm{rk}\, F_i = 0$.

Proof: For a *short* exact sequence $0 \to A \to B \to C \to 0$ of vector spaces over a field, the standard idea that any basis of A can be extended to a basis of B, with the (images of the) *new* elements forming a basis of $C \approx B/A$, proves the assertion in this case.

The general case is by induction: an exact sequence

$$0 \longrightarrow F_1 \longrightarrow \cdots \longrightarrow F_{n-1} \longrightarrow F_{n-1} \longrightarrow F_n \longrightarrow 0$$

with $n > 3$ can be broken into two smaller ones:

$$\begin{tikzcd}
0 \arrow[r] & \cdots \arrow[r] & F_{n-2} \arrow[rr] \arrow[dr] & & F_{n-1} \arrow[r] & F_n \arrow[r] & 0 \\
& & & X \arrow[ur] \arrow[dr] & & & \\
& & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

with X the image of F_{n-2} and the kernel of $F_{n-1} \to F_n$.

Then the two equations

$$\dim F_1 - \dim F_2 + \dim F_3 - \ldots + (-1)^{n-1} \dim X \ = \ 0$$

$$\dim X - \dim F_{n-1} + \dim F_n \ = \ 0$$

give the assertion, by subtracting or adding.

Remark: The same argument applies to exact sequences of *free modules* over a PID.

Remark: The same argument proves a counting result, namely, for an exact sequence of *finite* abelian groups,

$$0 \longrightarrow M_1 \longrightarrow \cdots \longrightarrow M_{n-1} \longrightarrow M_{n-1} \longrightarrow M_n \longrightarrow 0$$

$\prod_i |M_i|^{(-1)^i} = 1$, or, equivalently, $\sum_i (-1)^i \cdot \log |M_i| = 0$.

This bears on Herbrand-quotient issues.

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 $t\cdot\beta = N_k^K(\beta)$.

A formation ker/im 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 X to A factor:

$$\begin{tikzcd} A^G \arrow[r] & A \\ X \arrow[u, dashed, "\exists!"] \arrow[ur, "\forall"'] & \end{tikzcd} \qquad \text{(G acting trivially on X)}$$

The denominators in Theorem 90 are 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:

$$\begin{tikzcd} A_G \arrow[d, dashed, "\exists!"'] & A \arrow[l] \arrow[dl, "\forall"] \\ X & \end{tikzcd} \qquad (G \text{ acting trivially on } X)$$

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:

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

(Co-)homology quotients abstracting Theorem 90 are

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

Specifically, Theorem 90 says that for $A = K$ or $A = K^\times$ with K/k a finite separable extension,

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

In that situation, due to non-degeneracy of *trace* in separable extensions,

$$\frac{\ker(\sigma - 1)|_K}{\mathrm{im}\,t|_K} \;=\; \frac{k}{\mathrm{tr}_k^K K} \;=\; 0$$

and

$$\frac{\ker(\sigma - 1)|_{K^\times}}{\mathrm{im}\,t|_{K^\times}} \;=\; \frac{k^\times}{N_k^K K^\times} \;=\; \begin{cases} 1 & \text{(finite fields)} \\ \mathbb{Z}/[K:k] & \text{(unramified local)} \\ ?? & \text{(in general)} \end{cases}$$

Theorem: *(shortest long exact sequence)* A commutative diagram

$$\begin{tikzcd} & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\ 0 \arrow[r] & A \arrow[r] \arrow[d, "f"'] & B \arrow[r] \arrow[d, "f"'] & C \arrow[r] \arrow[d, "f"'] & 0 \\ 0 \arrow[r] & A' \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & C' \arrow[r] \arrow[d] & 0 \\ & 0 & 0 & 0 & \end{tikzcd}$$

with exact *rows* gives a long exact sequence

$$0 \to \ker f|_A \to \ker f|_B \to \ker f|_C \to \frac{A'}{fA} \to \frac{B'}{fB} \to \frac{C'}{fC} \to 0$$

Remark: The least obvious map is $\ker f|_C \longrightarrow A'/fA$.

Remark: The diagram is a short exact sequence of the *complexes* $0 \to A \to A' \to 0$, $0 \to B \to B' \to 0$, and $0 \to C \to C' \to 0$.

Least obvious part of the proof: The *connecting homomorphism* $\delta : \ker f|_C \longrightarrow A'/fA$ is not obvious. Recopying the diagram,

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r] \arrow[d, "f"'] & B \arrow[r] \arrow[d, "f"'] & C \arrow[r] \arrow[d, "f"'] & 0 \\
0 \arrow[r] & A' \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & C' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Given $f(c) = 0$, take $b \to c$. Then $f(b) \to f(c) = 0$, so there is $a' \to f(b)$. Put $\delta(c) = a'$. The rest of the proof is more natural. ///

Remark: The description of the connecting homomorphism is the *Snake Lemma*.

Example: Powers in $\mathbb{Z}_p^\times$, $p > 2$. Let $f(x) = x^n$, and consider

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & 1 + p\mathbb{Z}_p \arrow[r] \arrow[d, "f"'] & \mathbb{Z}_p^\times \arrow[r] \arrow[d, "f"'] & \mathbb{Z}/p^\times \arrow[r] \arrow[d, "f"'] & 0 \\
0 \arrow[r] & 1 + p\mathbb{Z}_p \arrow[r] \arrow[d] & \mathbb{Z}_p^\times \arrow[r] \arrow[d] & \mathbb{Z}/p^\times \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Let $\mu_n R$ be n^{th} roots of unity in R, and $U = 1 + p\mathbb{Z}_p$. The long exact sequence is (with multiplicative notation)

$$1 \to \mu_n U \to \mu_n \mathbb{Z}_p^\times \to \mu_n \mathbb{Z}/p^\times \to \frac{U}{U^n} \to \frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^n} \to \frac{\mathbb{Z}/p^\times}{(\mathbb{Z}/p^\times)^n} \to 1$$

For $p \nmid n$, ...

... with $p \not| n$ and $p > 2$ we understand n^{th} powers in U and in $\mathbb{Z}/p^\times$: on U the n^{th} power map is an isomorphism. Thus, (recopying)

$$1 \to \mu_n U \to \mu_n \mathbb{Z}_p^\times \to \mu_n \mathbb{Z}/p^\times \to \frac{U}{U^n} \to \frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^n} \to \frac{\mathbb{Z}/p^\times}{(\mathbb{Z}/p^\times)^n} \to 1$$

becomes

$$1 \to 1 \to \mu_n \mathbb{Z}_p^\times \to \mu_n \mathbb{Z}/p^\times \to 1 \to \frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^n} \to \frac{\mathbb{Z}/p^\times}{(\mathbb{Z}/p^\times)^n} \to 1$$

Two *isomorphisms*: whatever n^{th} roots of unity are in $\mathbb{Z}/p^\times$ lift to $\mathbb{Z}_p^\times$, and $x \in \mathbb{Z}_p^\times$ is an n^{th} power $\Leftrightarrow$ it is an n^{th} power mod p.

Remark: Obtaining n^{th} roots of unity in $\mathbb{Z}_p$ didn't seem to need Hensel's Lemma, only that $x \to x^n$ is an isomorphism on U.