Group Cohomology

I will define group cohomology H*(G, N) for any group G and any G-module N, and relate this to Hilbert Theorem 90.

The context is $Ext^*_R(M, N)$, for a ring R and two (left) R-modules M, N. This is a long theory to do everything, but one computation of Ext^*_R goes as follows:

(1) Choose a free R-module resolution complex $F_* \to M \to 0$ (resolution means exact)

(2) Form the cocomplex of abelian groups $Hom_R(F_*, N)$. Then $Ext^*_R(M, N)$ is the cohomology $H^*(Hom_R(F_*, N))$

(3) It is easy to see from half-exactness property of Hom that $H^0 = Hom_R(M, N)$.

(4) The codifferentials $Hom_R(F_k, N) \to Hom_R(F_{k+1}, N)$ are given by 'adjoints' of the differentials in F_*. Namely, the codifferential of an R-hom $z : F_k \to N$ is the composition $zd : F_{k+1} \to F_k \to N$.

In particular, z is a *k-cocycle* exactly when this composition $zd = 0$. The *k-coboundaries* are all compositions $F_k \to F_{k-1} \to N$, where first map is d.

(5) Take $M = \mathbb{Z}$ with *trivial G* action and take $R = \mathbb{Z}[G]$. Note R-modules and G-modules are the same thing. Then $H^*(G, N)$ is defined to be $Ext^*_{\mathbb{Z}[G]}(\mathbb{Z}, N)$.

(6) I will write down a free $\mathbb{Z}[G]$ module resolution $F_* \to \mathbb{Z} \to 0$.

As a free abelian group, F_k has $\mathbb{Z}$-basis $\{g_0 < g_1, \cdots g_k >\}$ with the $g_i \in G$. A plain bracket $< a, b, \cdots, x >$ is interpreted to have the identity $e \in G$ in front. The G-module structure is just multiply by g in front of the expression, so the new first term outside the bracket is gg_0. So a free $\mathbb{Z}[G]$ module basis of F_k is $\{< g_1, \cdots, g_k >\}$, the set of k-tuples of elements of G. When $k = 0$ this means $F_0 \simeq \mathbb{Z}[G]$, with $\mathbb{Z}$-basis $g < \varnothing >$ and $\mathbb{Z}[G]$-basis $\{< \varnothing >\}$. (A 0-*tuple* is a function $\varnothing \to G$, and there is one, the empty set, which is a subset of $\varnothing \times G$.)

(7) Here is a formula for $d : F_k \to F_{k-1}$, with *correct* signs.

$$d(g_0 < g_1, \cdots, g_k >) = g_0 g_1 < g_2, g_3, \cdots, g_k > - g_0 < g_1 g_2, g_3, \cdots, g_k > +$$

$$g_0 < g_1, g_2 g_3, g_4, \cdots, gk > - \cdots + (-1)^k g_0 < g_1, g_2, \cdots, g_{k-1} >$$

(Each summand amalgamates a $g_i g_{i+1}$, $0 \leq i \leq k - 1$, thus shortening the bracket, except at the end you just have the term $(-1)^k g_0 < g_1, \cdots, g_{k-1} >$ where g_k disappears. The signs alternate.)

Then d is extended $\mathbb{Z}$-linearly. Note d is a $\mathbb{Z}[G]$ module hom, the first coefficient g_0 sits in front of all terms in the sum, so d commutes with multiplying in front by some $g \in G$. By this observation, d is determined as a $\mathbb{Z}[G]$-module hom just by the formulas for $d(< g_1, \cdots, g_k >)$.

In lowest degrees $d_0(<\varnothing>) = 1 \in \mathbb{Z}$ and $d_1(< g_1 >) = g_1 <\varnothing> - <\varnothing>$ and $d_2(< g_1, g_2 >= g_1 < g_2 > - < g_1g_2 > + < g_1 >$, extended $\mathbb{Z}[G]$-linearly.

(8) One checks $dd = 0$. This is the associative law in G along with 'alternating signs'.

(9) The complex $F_* \to \mathbb{Z} \to 0$ is *exact* because, regarded as a chain complex of free abelian groups, Id and 0 are chain homotopic maps from the complex to itself, so the homology of this complex is 0. Specifically, define abelian group homs (not $\mathbb{Z}[G]$ homs) $h : F_k \to F_{k+1}$ by the formula

$$h(g_0 < g_1, \cdots, g_k >) =< g_0, g_1, \cdots, g_k >$$

extended $\mathbb{Z}$-linearly. We start here with $F_{-1} = \mathbb{Z}$ and $h(1) =<\varnothing>\in F_0$.

It is quite trivial to prove $dh + hd = Id - 0 = Id$. Namely $dh(g_0 < g_1, \cdots, g_k >)$ begins with the term $g_0 < g_1, \cdots, g_k >$ itself, and then you see all other terms in $(dh + hd)(g_0 < g_1, \cdots, g_k >)$ occur in canceling pairs.

(10) How do we describe the abelian groups $Hom_G(F_k, N)$ for a G module N? When $k = -1$ this means $H^0(G, N) = Hom_G(\mathbb{Z}, N) = N^G$, the G-invariant elements of N, since G acts trivially on $\mathbb{Z}$. On free modules over $\mathbb{Z}[G]$, the G-homs are determined by their values on a $\mathbb{Z}[G]$-basis. So for $k \geq 0$, a G-hom $F_k \to N$ is determined by any function $G \times \cdots \times G \to N$, the product taken k times. In the case of $F_0 = \mathbb{Z}[G] <\varnothing>\to N$, this just means choose an element of N, the image of the basis element $<\varnothing>$. Addition of the corresponding G-module homomorphisms $F_k \to N$ just corresponds to adding functions $G \times \cdots \times G \to N$ as N-valued functions.

(11) Referring to paragraph (4) and the formula for d in paragraph (7), we can write down what it means for a function $G \to N$ to represent a cocycle or a coboundary in $Hom_G(F_1, N)$.

For $z : F_1 \to N$ to be a cocycle, the composition $zd_2 : F_2 \to F_1 \to N$ must be 0. It suffices to compute the composition on $\mathbb{Z}[G]$-basis elements $< g_1, g_2 >$ of F_2. Since $d_2(< g_1, g_2 >= g_1 < g_2 > - < g_1g_2 > + < g_1 >$, the cocycle condition becomes

$$z(g_1g_2) = g_1z(g_2) + z(g_1).$$

Call these cocycle functions $Z^1(G, N)$, an additive subgroup of all functions $G \to N$.

For $z : F_1 \to N$ to be a coboundary, it must be a composition $z = cd_1 : F_1 \to F_0 \to N$. If $c <\varnothing>= b \in N$, then the corresponding coboundary is determined by

$$z < g >= cd_1(< g >) = c(g <\varnothing> - <\varnothing>) = gb - b$$

extended $\mathbb{Z}[G]$-linearly to $F_1 \to N$. Call these coboundary functions $B^1(G, N)$.

We see that

$$H^1(G, N) = \frac{Z^1(G, N)}{B^1(G, N)},$$

a very explicit description of H^1, but in the context here of developing an approach to group cohomology $H^*(G,N)$ in all degrees, not just an isolated H^1 thing.

(12) Suppose G is a *finite cyclic* group, $G = \{g, g^2, \cdots, g^n = 1\}$. We determine the 1-cocyles $z : G \to N$. Taking $v = 1$ in the cocycle condition $z(uv) = uz(v) + z(u)$, we see that always $uz(1) = 0 \in N$, hence $z(1) = 0 \in N$. Say $z(g) = a \in N$. We use the cocycle condition to compute $z(g^2) = gz(g) + z(g) = ga + a$. Continuing inductively $z(g^k) = \sum_{i=0}^{k-1} g^i a$. But we must have $0 = z(g^n) = \sum_{i=0}^{n-1} g^i a \in N$. Any $a \in N$ satisfying this last formula defines a cocycle, so $Z^1(G,N) = ker(\sum_0^{n-1} g^i) \subset N$

The 1-coboundaries are the functions $z(g^i) = g^i b - b$, for any fixed $b \in N$. In particular, the corresponding cocycle element is $a = z(g) = gb - b$.

(13) Suppose $F \subset E$ is a finite Galois extension with *cyclic* Galois group $G = Gal(E/F)$. Take $N = (E, +)$, the additive group, which is a G module. Then paragraph (12) explains why in the cyclic case

$$Z^1(G,E) = \{a \in E \mid Trace_{E/F}(a) = 0\} \text{ and } B^1(G,E) = \{gb - b \mid b \ \in E\}$$

Take $N = (E^*, \cdot)$, the muliplicative group, which is also a G module. Since the group operation in N is multiplication in E, paragraph (12) says that

$$Z^1(G,E^*) = \{a \in E^* \mid Norm_{E/F}(a) = 1\} \text{ and } B^1(G,E^*) = \{\frac{gb}{b} \mid b \in E^*\}.$$

(14) It turns out to be a consequence of linear independence of characters that for ANY finite Galois extension $F \subset E$ with $G = Gal(E/F)$ one has $H^1(G,E) = 0$ and $H^1(G,E^*) = 0$. A proof is on pages 302-303 of Lang. It is not hard.

Hilbert Theorem 90 says that for cyclic Galois extensions, any trace 0 element has the form $gb - b$, and any norm 1 element has the form gb/b. Therefore, by paragraph (13), we see that Hilbert Theorem 90 is a special case of a much more general cohomology vanishing theorem.

(15) Here was my goal in this discussion: Review some things about *Ext* and cohomology of groups in general, describe a classical explicit free resolution of $\mathbb{Z}$ over the group ring $\mathbb{Z}[G]$, make clear what are the 1-cocycles and 1-coboundaries with coefficients in N for this resolution, compute 1-cocycles and 1-coboundaries when G is a finite cyclic group, state the general vanishing of H^1 for Galois groups acting on a field E, and point out that Hilbert Theorem 90 is exactly this H^1 cohomology vanishing theorem for cyclic Galois extensions.