Lecture 2-7: Restriction and corestriction maps; applications of H^1

February 7, 2025

Continuing from last time, I now address the problem of computing the cohomology of a group. The main tool is to relate this to the cohomology of a smaller group.

Definition, p. 805

Given groups G, G', modules A, A' over G, G', respectively, and a pair of homomorphisms $\phi : G' \to G, \psi : A \to A'$, we say that ϕ, ψ are *compatible* if $\psi(\phi(g')a) = g'\psi(a)$ for $g' \in G', a \in A$.

An easy example is the case $G = G', \phi = 1$, and $\psi : A \to A'$ a G-module map. Given compatible maps ϕ, ψ we get a natural map λ_n from the cochain group $C^n(G, A)$ defined last time to $C^n(G', A')$, by multiplying on the left by ψ and on the right by n copies of ϕ. These maps commute with the coboundary operators, so induce well-defined homomorphisms from $H^n(G, A)$ to $H^n(G', A')$. The two most important examples are

- The *restriction homomorphism* (p. 805) attached to a subgroup H, taking ϕ to be the inclusion of H into G and ψ to be the identity map. Here we get a map Res from $H^n(G, A)$ to $H^n(H, A)$, which on the cochain level just restricts maps from G^n to H^n.

- The *corestriction map* (p. 806), again attached to a subgroup H. Fixing representatives $g_1, \ldots, g_m$ of the left cosets of H in G, we get a map $\psi : M_H^G(A) \to A$ sending f to $\sum_{i=1}^{m} g_i \cdot f(g_i^{-1})$. Since f is an H-module map, this last sum does not depend on the choice of coset representatives g_i; one easily checks that it is a G-module map, so that it is compatible with the identity map on G. Since we have $H^n)(G, M_H^G(A)) \cong H^n(H < A)$ by Shapiro's Lemma, we get a map Cor: $H^n(H, A) \to H^n(G, A)$ such that if $f \in \hom_{\mathbb{Z}H}(P_n, A)$ represents a cohomology class in $H^n(H, A)$, then $\mathrm{Cor}(f) \in \hom_{\mathbb{Z}G}(P_n, A)$ represents its image in $H^n(G, A)$, where

$$\mathrm{Cor}(f)(p) = \sum_{i=1}^{m} g_i f(g_i^{-1} p), p \in P_n$$

In particular, for $n = 0$, this map just averages an H-fixed element of A over G to produce a G-fixed element, as in the proof of Maschke's Theorem last quarter.

The main payoff from the corestriction map emerges in the following result.

Proposition 26, p. 807

If H has index m, then the composite Cor$\circ$Res is multiplication by m (as a map from $H^n(G, A)$ to itself).

This follows at once from the explicit formula above for both Res and Cor. If $f \in \hom_{\mathbb{Z}H}((P_n, A)$ happens to lie in $\hom_{\mathbb{Z}G}(P_n, A)$, then all terms $g_i f(g_i^{-1} p)$ are equal to $f(p)$, so that Cor$\circ$Res$(f) = mf$.

In particular, since the cohomology of the trivial group is 0 in all positive degrees, we deduce that if the group G has order m, then $mH^n(G, A) = 0$ for all G-modules A and all $n > 0$ (Corollary 27, p. 807). Combining with the earlier observation that $rH^n(G, A) = 0$ for all $n \geq 0$ if $rA = 0$, we get a simple criterion for the cohomology groups $H^n(G, A)$ to be 0:

Corollary 28, p. 807

If G has order relatively prime to the least positive r with $rA = 0$, then $H^n(G, A) = 0$ for all $n > 0$.

I mention in passing two other examples of compatible maps. Any G-module map $A \to A'$ is compatible with the identity map on G, so we get a natural homomorphism from $H^n(G, A)$ to $H^n(G, A')$ for any n. Also, if H is a normal subgroup of G and A is a G-module, then the subgroup A^H is a module for the quotient group G/H in a natural way; then the projection map from G to G/H is compatible with the inclusion of A^H into A.. We therefore get an inflation homomorphism Inf: $H^n(G/H, A^H) \to H^n(G, A)$ for all n (p. 806).

Next I turn to an interpretation of the first cohomology group $H^1(G, A)$. From the bar resolution (used for the first time) one deduces that if $f \in C^1(G, A)$, then f is a cocycle if and only if $df(g, h) = gf(h) + f(g) - f(gh) = 0$ or $f(gh) = f(g) + gf(h)$, writing the group operation in A additively. Such an f is often called a crossed homomorphism from G into A (p. 814), since if the action of G on A is trivial, then a crossed homomorphism is just a homomorphism from G into A. Similarly, f is a coboundary if and only if there is $a \in A$ such that $f(g) = ga - a$ for all $g \in G$. A crossed homomorphism of this type is called principal. Thus we can now describe $H^1(G, A)$ as the quotient of the group of crossed homomorphisms by the subgroup of principal ones. If the action of G on A is trivial, then there are no nonzero coboundaries and $H^1(G, A) \cong \mathrm{hom}(G, A)$, the additive group of homomorphisms of G into A.

An interesting example arises from Galois theory. Let L be a finite Galois extension of a field K with Galois group G. Then G acts on the (abelian) multiplicative group L^* by automorphisms.

Hilbert's Theorem 90, p. 814

With notation as above, we have $H^1(G, L^*) = 0$.

Indeed, if f is a crossed homomorphism from G into L^*, then the linear independence over L of automorphisms of L shows that there is $y \in L^*$ with $x = \sum_{g \in G} f(g)gy \neq 0$. For $h \in G$ we then have $hx = \sum_g h(f(g))(hg)y = \sum_g f(hg)f(h)^{-1}(hg)y = (\sum_g f(hg)(hg)y)^{-1}f(h)^{-1}) = (\sum_g f(g)gy))f(h)^{-1} = xf(h)^{-1}$, whence f is principal (using multiplicative notation for L^*).

To interpret this result in Galois-theoretic terms I need to restrict to a special case and make a definition. Recall that the norm $N(x)$ of any $x \in L$ is the product $\prod_g gx$ of its images under G. We have $N(x) = 0$ if and only if $x = 0$ and $N(xy) = N(x)N(y)$. Now specialize to the case where $G = \langle g \rangle$ is cyclic, say of order n.

Then $N(x) = \prod_{i=0}^{n-1} g^i x$. Bearing in mind the formula given last time for the cohomology of a cyclic group (and the multiplicative notation which we are using for L^*), we see that $H^1(G, L^*)$ can be interpreted in this case as the subgroup of L^* consisting of elements of norm 1, modulo the subgroup of elements of the form gx/x for some $x \in L^*$.

Hence every element of L^* of norm 1 is of the form gx/x for some $x \in L^*$. This last statement is also often called Hilbert's Theorem 90, since it is what he actually proved in 1897. Now specialize even further, down to the case where K contains $n = |G|$ distinct nth roots of 1. If $\alpha \in K$ is a primitive such root, then it is clear that $N(\alpha) = 1$, whence there is $\beta \in L$ with $g\beta = \alpha\beta$ and $\beta^n = c \in K$. We then saw previously that $L = Kk(\beta)\beta^n \in K$. We conclude that any cyclic Galois extension of degree n of a field K with n distinct nth roots of 1 is generated by a single nth root of an element of K. This was a key step in the proof of the Galois criterion for solvability by radicals.

There is an additive version of the norm called the trace: If L is a finite Galois extension of K with Galois group G, then the trace $T(x) = \sum gx$ is the sum of the Galois conjugates of x; we once again have $T(x) \in K$, but this time $T(x+y) = T(x) + T(y)$. Hilbert's Theorem 90, now applied to the additive action of G on L, says that given any map $f : G \to L$ with $f(gh) = f(g) + gf(h)$ there is $z \in L$ with $f(g) = gz - z$. In particular, if G is cyclic, say generated by g, and if $T(x) = 0$ for some $x \in L$, then $x = gy - y$ for some $y \in L$. Specializing even further, down to the case where the degree $[L : K]$ is a prime p and K has characteristic p, the element 1 has trace 0, so there is $\beta \in L$ with $g\beta = \beta + 1$, whence $\beta^p - \beta = c$ is fixed by G and lies in K. The Galois conjugates $\beta + i$ of β are again the roots of its minimal polynomial over K, which must be $x^p - x - c$, and β generates L over K. Note that in this case L cannot possibly be a pth root extension, since no such extension is ever separable in characteristic p.

Returning now to the general situation of a finite group G acting on an abelian group A by automorphisms, recall from last quarter that we have the semidirect product $H = A \ltimes G$, a group with A as an abelian normal subgroup on which G has the given automorphism action. The group G is then a subgroup of H complementary to A, so that $A \cap G = 1$ and $H = AG$. We might ask what other complements G' there are (if any) to A inside H, so that G' maps isomorphically onto G under the projection map $H/A \to G$. Any such complement replaces $g \in G$ by $g' = f(g)g$ for some $f : G \to A$. The condition that $g'h' = (gh)'$ then amounts exactly to the crossed homomorphism condition on f, while a coboundary replaces G by its conjugate $a^{-1}Ga$ for fixed $a \in A$.

We conclude that

Proposition 33, p. 820

With notation as above, A-conjugacy classes of complements to A in H are in bijection to elements of $H^1(G, A)$.

In particular, if A is also finite and has order relatively prime to that of G, then any two complements of A in H are conjugate under A.