Lecture 4-29: Restriction, corestriction, and H^1

April 29, 2024

We exhibit some important maps relating the cohomology of a group G and that of its subgroups H; these lead to an important constraint on the cohomology of G. For every G-module A we write down explicit equations describing the first cohomology group $H^1(G, A)$ and relate this group to group extensions of A by E

We begin with a definition. Given finite groups G, G', modules A, A' over G, G', and group homomorphisms $\phi : G' \to G, \psi : A \to A'$, we say that ϕ and ψ are *compatible* if $\psi(\phi(g')a) = g'\psi(a)$ for $g' \in G', a \in A$. If this holds then ϕ and ψ induce homomorphisms $\lambda_n : C^n(G, A) \to C^n(G', A')$ for all n, which commute with the coboundary maps, so that they map cocycles to cocycles and coboundaries to coboundaries. Hence we get a homomorphism $\lambda_n : H^n(G, A) \to H^n(G', A')$. As a simple example, any G-homomorphism $A \to A'$ is compatible in this sense with the identity map on G, so we get a natural map from $H^n(G, A)$ to $H^n(G, A')$.

In particular, if A is a G-module, then A is also a module over any subgroup H of G; since the inclusion of H into G and the identity map from A to itself are compatible in this sense, we get a restriction homomorphism Res: $H^n(G, A) \to H^n(H, A)$ for $n \geq 0$, which on the cochain level just restricts a map in $C^n(G, A)$ to H^n (DF, p 806). If H is a normal subgroup of G and A is a G-module, then the H-fixed subgroup A^H of A is a module for the quotient group G/H. The projection $G \to G/H$ and the inclusion of A^H into A are then compatible, so that we get an inflation homomorphism Inf: $H^n(G/H, A^H) \to H^n(G, A)$ for $n \geq 0$.

Now let H be a subgroup of G of index m and A a G-module. Let $g_1, \ldots, g_m$ be representatives for the left cosets of H in G. Define a map $\psi : M_H^G(A) \to A$ via $f \mapsto \sum_{i=1}^{m} g_i \cdot f(g_i^{-1})$. If we change any coset representative g_i to $g_i h$ then $(g_i h) f((g_i h)^{-1} = g_i h f(h^{-1} g_i^{-1}) = g_i h h^{-1} f(g_i^{-1}) = g_i f(g_i^{-1})$. so the map ψ is independent of the choice of coset representatives; it is also easily seen to be a G-homomorphism. By Shapiro's Lemma we have an isomorphism $H^n(G, M_H^G(A)) \cong H^n(H, A)$, so by composing the two homomorphisms we get the corestriction homomorphism Cor: $H^n(H, A) \to H^n(G, A)$ (DF, p. 806). For a cocycle $f \in \hom_{\mathbb{Z}H}(P_n, A)$ representing a cohomology class $c \in H^n(H, A)$ (arising from a projective resolution $\{P_n\}$ of $\mathbb{Z}$ over H) we have that $\text{Cor}(f) \in \hom_{\mathbb{Z}G}(P_n, A)$ is defined by

$$\text{Cor}(f)(p) = \sum_{i=1}^{m} g_i f(g_i^{-1} p).$$

Then we have

Proposition 26, DF, p. 807

If H is a subgroup of G of index m, then the composite Cor$\circ$Res is multiplication by m.

This follows at once from the formula for $\text{Cor}(f)(p)$ given above, since if f is a G-homomorphism, then all terms in the sum for $\text{Cor}(f)(p)$ are equal to $\text{Cor}(f)(p)$. As an immediate consequence (taking $H = 1$) we get that given a finite group G of order m we have $mH^n(G, A) = 0$ for all $n \geq 1$, so that $H^n(G, A)$ is a torsion abelian group. Moreover, if A is finite abelian with $|A|$ and m relatively prime, then it follows from this and a previous result that $H^n(G, A) = 0$ for all $n \geq 1$.

Turning now to the first cohomology group $H^1(G, A)$, it follows from the definitions of $Z^1(G, A)$ and $B^1(G, A)$ that $f : G \to A$ is a cocycle if and only if $f(gh) = f(g) + gf(h)$ for all $g, h \in G$ (using additive notation for A). We call such f crossed homomorphisms); note that if G acts trivially on A, then crossed homomorphisms are just ordinary group homomorphisms from G into A. Plugging in $g = 1$, we see that this condition forces $f(1) = 0$. A 1-cochain f is a coboundary if and only if there is $a \in A$ with $f(g) = ga - a$; crossed homomorphisms with this property are called principal.

As an example, let G be the Galois group of a finite Galois extension K of F; take A to be the multiplicative group K^*. A simple calculation (see DF, p. 814) shows that $H^1(G, K^*) = 0$. (The same result holds even for infinite Galois extensions, but it does *not* extend to the higher cohomology groups $H^n(G, K^*)$). In particular, if G is cyclic with generator σ, then in view of a previous computation of H^1 for cyclic groups this computation shows that $\alpha \in K^*$ has norm 1 (that is, the product of its conjugates under G is 1) if and only if $\alpha = \sigma(\beta)/\beta$ for some $\beta \in K^*$. If the field F has m distinct mth roots of 1, where $m = |G|$, then a primitive mth root ϵ_m of 1 in F has norm 1, whence there is $\beta \in K^*$ with $\sigma(\beta) = \beta\epsilon_m$. It easily follows that K is an mth root extension of F (it is generated by β and $\beta^m \in F$).

This is an important step in the proof that in characteristic 0, a polynomial with solvable Galois group is solvable by radicals. The corresponding fact in characteristic $p > 0$ is that a Galois extension K of degree p is an extension by some β with $\beta^p - \beta \in F$; here one looks at the cohomology group $H^1(G, K)$ of G with coefficients in the *additive* group K. In this case a polynomial with solvable Galois group need *not* be solvable by radicals alone.

Our main application of $H^1(G, A)$ is to group extensions; the cohomological theory of these is quite similar to that of module extensions. Given a group G and a G-module A, an extension of G by A is a short exact sequence $1 \to A \to E \to G \to 1$ of groups. (Note that exactness forces the image of A in E to be a normal subgroup.) We identify two extensions $1 \to A \to E \to G \to 1$ and $1 \to A \to E' \to G \to 1$ whenever there is an isomorphism $\pi : E \to E'$ restricting to the identity map on the copy of A sitting inside E and commuting with the projection maps $\pi : E \to G, \pi' : E' \to G$. For now we consider only split extensions, that is, ones for which there is a homomorphism $\sigma : G \to E$ such that the composite $\pi\sigma$ is the identity on G. Such a σ is called a splitting and its image a complement to A in E.

In this case we identify E with the semidirect product $A \rtimes G$, consisting of all ordered pairs $(a, g) \in A \times G$ with multiplication given by $(a, g)(b, h) = (a + gb, gh)$ (recalling once again that the group operation is written multiplicatively in E and G but additively in A). Now consider the set of all splittings σ. Any such sends $g \in G$ to $(f(g), g)$ for some $f : G \to A$; since $(f(g), g)(f(h), h) = (f(g) + gf(h), gh)$ the condition that σ be a homomorphism is equivalent to requiring that $f \in Z^1(G, A)$. Composing σ with conjugation by $(a, 1)$ for any $a \in A$ then amounts to replacing f by $f + a - ga$, that is, altering f by a 1-coboundary.

Reformulating the above discussion slightly, we obtain

Theorem, DF, Proposition 33, p. 820

Given a semidirect product $E = A \rtimes G$ (with fixed action of G on A) there is a bijection between E-conjugacy classes of complements to A in E and $H^1(G, A)$.

Proof.

A complement to A in E necessarily takes the form $\{(f(g), g); g \in G\}$ for some $f : G \to A$; we have seen that such a function must be a 1-cocycle. As such a complement is stable under conjugation by any of its elements, its E-conjugacy classes are the same as its A-conjugacy classes, which we have shown to be in bijection to $H^1(G, A)$. □

For example, let $G = \mathbb{Z}/2\mathbb{Z}$ act on $A = \mathbb{Z}/4\mathbb{Z}$ by inversion (the unique nontrivial element of G sends every element of A to its inverse). The semidirect product $E = A \rtimes G$ is then the dihedral group D of order 8; the subgroup A consists of the rotations in D. The complements of A in E are then the cyclic subgroups generated by reflections in D. There are two conjugacy classes of such reflections; accordingly, $H^1(G, A)$ is cyclic of order 2. This agrees with the earlier computation of the cohomology groups of a cyclic group. This example is discussed on p. 820.

As an immediate consequence we get

Corollary, DF, p. 821

Given a semidirect product $E = A \rtimes G$ with A abelian and the order of G relatively prime to that of A, all complements of A in E are A-conjugate.

This follows since we saw above that $H^n(G, A) = 0$ for $n \geq 0$ in this situation.