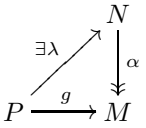
A Layman's Practical Crash Course on Group/Galois Cohomology

Frank Gounelas - 22/1/2009

We want to start with a group G and an abelian G-module M (that is a $\mathbb{Z}[G]$-module M)[1] and to find a series of *simple enough* groups (the cohomology groups) which will encode in some sense properties not only of the action of G on M but also of G and M themselves. How exactly these groups are used and what they imply for arithmetic algebraic geometry will be elaborated more in the seminar. For now, we start with definitions. A projective module P is one such that for every surjective homomorphism $\alpha : N \to M$, the map $\mathrm{Hom}_G(P, N) \to \mathrm{Hom}_G(P, M)$ given by $\lambda \mapsto \alpha \circ \lambda$ is surjective:



Projective modules are in a sense quite close to free modules, as P is a projective module if and only if there exists a module M and a free module F such that $P \oplus M \cong F$ (†). Now, consider a sequence of homomorphisms between infinitely many R-modules

$$\cdots \xrightarrow{d^{i-1}} A^i \xrightarrow{d^i} A^{i+1} \xrightarrow{d^{i+1}} A^{i+2} \xrightarrow{d^{i+2}} \cdots$$

We say that this forms a *cohomological complex* if $d^{i+1} \circ d^i = 0$ for all i, and that it's an *exact sequence* if $\operatorname{im} d^i = \ker d^{i+1}$. Obviously any exact sequence is a cohomological complex. Now, for a ring R and an R-module A, we say that the exact sequence $\cdots \to P_1 \to P_0 \to A \to 0$ is a *projective resolution of* A if the P_i are all projective R-modules. Given an A it is not hard to construct a projective resolution. One can for example take $P_0 = \oplus_{a \in A} R$ as the free R-module which is an infinite direct sum of copies of R indexed by elements of A. This gives a clear surjection $p_0 : P_0 \to A$ and P_0 is free and so is projective from (†). Next, inductively, when P_i, p_i are defined, one does the same thing as above, but for $\ker p_i$ instead of A, to construct P_{i+1}, p_{i+1}. Now, to construct the cohomology groups $\mathrm{H}^i(G, M)$, we pick any projective resolution $\cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} \mathbb{Z} \to 0$ of $A = \mathbb{Z}$ and form the complex (it's not exact!)

$$\mathrm{Hom}_G(\mathbb{Z}, M) \xrightarrow{d^{-1}} \mathrm{Hom}_G(P_0, M) \xrightarrow{d^0} \mathrm{Hom}_G(P_1, M) \xrightarrow{d^1} \mathrm{Hom}_G(P_2, M) \xrightarrow{d^2} \cdots \tag{1}$$

where $d^i : \lambda \mapsto \lambda \circ p_{i+1}$. For $i \geq 0$ define the *i-th cohomology group* $H^i(G, M) = \ker(d^i)/\operatorname{im}(d^{i-1})$. The magic behind this definition is that not only can we always derive one such complex since there's always a projective resolution of $\mathbb{Z}$, but also that even if we picked a different resolution, the cohomology groups would be isomorphic (needs proof but isn't too hard)! The above construction can be made much more explicit if we consider the resolution $\cdots \xrightarrow{p_2} \mathbb{Z}[G^2] \xrightarrow{p_1} \mathbb{Z}[G] \xrightarrow{p_0} \mathbb{Z} \to 0$ where $p_i(\sigma_0, \ldots, \sigma_i) = \sum_{j=1}^{i} (-1)^j (\sigma_0, \ldots, \sigma_{j-1}, \sigma_{j+1}, \ldots, \sigma_i)$, that is we remove the j-th entry for every summand. In this setting, applying the same Hom_G construction as before, one calls elements of $\mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], M)$ the *i-cochains*, whereas $\ker(d^i)$ are the *i-cocycles* and $\operatorname{im}(d^{i-1})$ the *i-coboundaries*. If we change the maps p_i slightly (it's slightly more cumbersome to write down, but following the same ideas) one derives the *inhomogeneous cochains construction*. Here, we can explicitly say what the kernel and image of the d^i's is. The easiest cases are

$$\mathrm{H}^0(G, M) = A^G = \{a \in A : g \cdot a = a \ \forall g \in G\} \tag{2}$$

$$\mathrm{H}^1(G, M) = \{s \mapsto a_s : G \to A | a_{st} = a_s \cdot s(a_t)\} \,/\, \{\exists a : s \mapsto a^{-1} s(a)\} \tag{3}$$

Theorem. ***(Hilbert's 90 Original)*** *Let L/K be a finite Galois extension such that $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$ is a cyclic group. For $a \in L$ we have that $\mathrm{N}_{L/K}(a) = 1$ if and only if $a = b/\sigma(b)$ for some $b \in L$.*

Theorem. ***(H90 General)*** *Let L/K be any finite Galois extension. Then using (3) prove $\mathrm{H}^1(\mathrm{Gal}(L/K), L^\times) = 0$.*

[1] Remember that for a ring R and a group G, the *group ring* $R[G]$ is defined as the set $\{\sum r_i g_i : r_i \in R, g_i \in G\}$ of *finite* R-linear combinations of elements of G with the obvious addition, and R-linear multiplication in G: e.g. $(r_1 g_1 + r_2 g_2) * (r_3 g_3) = (r_1 r_2) g_1 \cdot g_3 + (r_1 r_3) g_2 \cdot g_3$ and so on...

Proof. Let $G = \mathrm{Gal}(L/K)$ and consider a cocycle $s \mapsto a_s$ in $H^1(G, L^\times)$. For $c \in L$, consider the Poincaré series $b = \sum_{s \in G} a_s \cdot s(c)$. First, prove that the elements of G are linearly independent over L (Hint: By contradiction on the minimality of n in an assumed $a_1\sigma_1 + \ldots + a_n\sigma_n = 0$ with $a_i \neq 0$, but don't get too bogged down with this as it doesn't need cohomology!). Using this fact we can pick a c such that $b \neq 0$. Apply s to b and show that a_s is a coboundary. *ŏ.ĕ.δ.*

Proposition. *Calculate all the cohomology groups of an abelian $\mathbb{Z}[\mathbb{Z}]$-module A using the definition after (1) only.*

Proof. First check that for σ a generator of the cyclic group $\mathbb{Z}$, we have that $0 \xrightarrow{p_2} \mathbb{Z}[\mathbb{Z}] \xrightarrow{p_1} \mathbb{Z}[\mathbb{Z}] \xrightarrow{p_0} \mathbb{Z} \to 0$, where p_1 is multiplication by $\sigma - 1$ and p_0 maps σ to 1, is a projective resolution of $\mathbb{Z}$. Next, apply the $\mathrm{Hom}_{\mathbb{Z}[\mathbb{Z}]}(-, A)$ functor to the resolution and write down explicitly the maps d_i between the hom-groups. Noting that $\mathrm{Hom}_G(\mathbb{Z}, B) \cong B^G$ for any group G and G-module B, write down explicitly the kernel and image of the necessary d_i's and calculate the relevant quotients giving rise to the cohomology groups. *ŏ.ĕ.δ.*

As you may have guessed, Galois cohomology is just the cohomology of $G = \mathrm{Gal}(L/K)$-modules M for some Galois field extension L/K. This cohomology can still be formed using explicit resolutions and the cochain constructions as above, but it has more properties that just simple group cohomology. Namely, we know that G is a profinite group and hence a topological group (with the profinite topology). The cocycles and coboundaries are thus not only as above, but also continuous maps in this topology. What's even more striking is that for G a profinite group and M a G-module, we have that $H^p(G, M)$ is finite for $p \geq 1$. More about Galois cohomology in the seminar.