Lecture 3-12: Review, part 2

March 12, 2025

Today I will concentrate on group cohomology and its applications, particularly to finite-dimensional central simple algebras over a field.

If G is a finite group and A is a G-module (that is, an abelian group on which G acts linearly), then $H^n(G, A)$, the nth cohomology group of G with coefficients in A, is defined to be $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$, the nth Ext group of the trivial module $\mathbb{Z}$ over the (integral) group ring $\mathbb{Z}G$ with coefficients in A. It can be computed by taking a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module (for example the bar resolution), taking homomorphisms of each term in to A, and then taking the cohomology groups of the resulting cochain complex.

Using this definition, it is easy to compute the cohomology groups $H^n(\mathbb{Z}_n, A)$of the cyclic group $\mathbb{Z}_n$ of order n. Letting σ be a generator of this group and writing $N = 1 + \sigma + \ldots + \sigma^{n-1}$ we have $H^0(G, A) = A^G, H^n(G, A0 = {}_NA/(\sigma - 1)A$ for odd $n \geq 1, H^n(G, A) = A^G/NA$ for even $n \geq 2$, where A^G denotes the set of G-fixed vectors in A and ${}_NA$ denotes the set of vectors in A sent to 0 by N. (In fact the formula $H^0(G, A) = A^G$ holds for any group G and module A.) This basic example should always be kept in mind. Two very useful general facts are that $|A|H^n(G, A) = 0$ for $n > 0$ if A is finite of order $|A$ and $|G|H^n(G, A) = 0$ for $n > 0$ if $|G|$ is the order of G. In particular, if A is finite and of order relatively prime to that of G, then $H^n(G, A) = 0$ for all $n > 0$.

In view of the bar resolution, one can also write down formula for $H^n(G, A)$ directly, making no reference to Ext groups or projective resolutions. The detailed formula are not so important, but two special cases are. First of all, $H^1(G, A)$ may be identified with the group of crossed homomorphisms $f : G \to A$, satisfying $f(g_1 g_2) = f(g_1) + g_1 \cdot f(g_2)$, modulo the subgroup or principal crossed homomorphisms, of the form $f(g) = g \cdot a - a$ for some fixed $a \in A$. Secondly, $H^2(G, A)$ may be identified with the group of factor sets $f : G^2 \to A$, such that $f(g, h) + f(gh, k) = g \cdot f(h, k) + f(g, hk)$, modulo coboundaries, of the form $b(g, h) = \ell(g) + g\ell(h) - \ell(gh)$ for some $\ell : G \to A$. Any factor set f can be normalized, so that it is replaced by another factor set f' differing from it by a 1-coboundary, such $f'(1, g) = f'(g, 1) = 1$ for all $g \in G$. In these formulas the group operation in A is written additively throughout.

The formulas for $H^1(G, A)$ and $H^2(G, A)$ lead directly to group-theoretic interpretations of these cohomology groups: $H^1(G, A)$ parametrizes A-conjugacy classes of complements of A in a semidirect product $E = A \ltimes G$, where G acts on A in E according to the specified action. Similarly, $H^2(G, A)$ parametrizes equivalence classes of extensions of G by A, that is, short exact sequences of groups of the form $1 \to A \to E \to G \to 1$. Recall that the notion of equivalent extension refers to the entire exact sequence and *not* just the isomorphism class of the middle group E.

Galois theory and group cohomology come together in an especially beautiful way in the theory of finite-dimensional central simple algebras over a fixed field F, equivalence classes of these being parametrized by the Brauer group of F defined last quarter. Here I developed the theory more deeply than in the text, taking the time to prove some assertions only stated there. Specifically, any central simple algebra over F is equivalent to a central division algebra over F and then in turn is equivalent to an algebra A over F admitting a maximal subfield K which is finite Galois over F, such that the degree $[A : F] = [K : F]^2$. Any such algebra A admits a basis over K indexed by the Galois group G of K over F, such that basis elements e_g multiply in A according to a factor set $f \in H^2(G, K^*)$, so that $e_g e_h = f(g, h) e_{gh}$. The element e_g acts on K by conjugation as g does.

Given two central simple algebras A, A' over F with the same maximal subfield K, addition of their respective factor sets f, f' corresponds to taking the equivalence class $[A \otimes_F A']$ of their tensor product $A \otimes A'$, this latter operation in turn corresponding to multiplication in the Brauer group. In this way one captures a piece $H^2(G, K^*)$ of $\mathrm{Br}(F)$, where G is the Galois group of K over F; but in order to capture the whole Brauer group one must take into account all finite Galois extensions of F simultaneously. This is done by looking at the inverse limit of Galois groups of finite extensions of F, partially ordering such extensions by inclusion.

A very important special case is that of $F = \mathbb{R}$. Here F admits just two Galois extensions, namely itself and $\mathbb{C}$, the latter having cyclic Galois group of order two. Accordingly there are just two central division algebras over F up to isomorphism, namely F itself and the ring H of quaternions, the latter corresponding to the nontrivial element of $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{C}^*)$. Over $\mathbb{Q}$, by contrast, one gets not just ring of quaternions, but many, one for each choice of nonzero $a, b \in -\mathbb{Q}^+$ such that ba^{-1} is not a square in $\mathbb{Q}$. Such rings are generated by two elements x, y over $\mathbb{Q}$ such that $x^2 = a, y^2 = b, xy = -yx$.

Thus the Brauer group $\mathrm{Br}(\mathbb{R})$ is cyclic of order two; of course the Brauer group of any algebraically closed field F is trivial. The Brauer group is also trivial for finite fields F and in a few other cases. If it is finite but not trivial, then it must be cyclic of order two, since a well-known theorem asserts that if a field F is such that its algebraic closure K is a finite nontrivial extension of F, then in fact K is generated over F by a square root of -1.

Next time I will review Dedekind domains, which are the ring-theoretic analogues of finite Galois extensions K of $\mathbb{Q}$. More precisely, the Dedekind domain $\mathcal{O}_K$ corresponding to the Galois extension K consists of all elements of K integral over $\mathbb{Q}$ (roots of a monic polynomial in $\mathbb{Z}[x]$).