Lecture 2-12: H^2 and central simple algebras

February 12, 2025

Last time I showed how the second cohomology group $H^2(G, A)$ can be used to study group extensions of a finite group G by an abelian group A on which it acts, using factor sets. There is another context in which factor sets arise, namely that of central division algebras finite-dimensional over a field F. I first discussed such algebras in the lecture on January 31. As I did then, I will assume now for simplicity that F has characteristic 0 (though the results extend to any field).

On January 31 I showed that given any central division algebra D over F, there is a matrix ring $D' = M_s(D)$ over D for some s containing a Galois extension K of F, say with Galois group G. I also showed that for any $g \in G$ there is a unit $e_g \in D'$, unique up to multlplication by an element of K^*, such that conjugation by e_g preserves K and acts on it by the automorphism g. The dimension of D' over F is equal to the square n^2 of the order n of G, which in turn of course equals the degree $[K : F]$.

As noted in January, the elements e_g form a K-basis of D' and knowledge of the products $e_g e_h$ completely determines the structure of D'. Since K is a maximal subfield of D' and thus equal to its own centralizer, and since conjugation by either $e_g e_h$ or e_{gh} acts on K by the automorphism $gh \in G$, we must have $e_g e_h = f(g,h)e_{gh}$ for some $f \in C^2(G, K^*)$, where G acts on the multiplicative group K^*. Exactly as in the case of group extensions last time, the function f must be a 2-cocycle; multiplying each e_g by $\ell(g)e_g$ for some $\ell \in C^1(G, K^*)$ amounts to replacing f by itself plus a 1-coboundary. We can normalize f by taking $e_1 = 1$, so that $f(1,g) = f(g,1) = 1$ for all $g \in G$.

As with group extensions, all of the above steps to get from a central simple algebra to a cohomology class through a factor set are reversible. Given any Galois extension K of F with Galois group G and a factor set $f \in H^2(G, K^*)$, one can write down formal elements e_g for $g \in G$, multiply them by the rule $e_g e_h = e_{gh}, e_g k e_g^{-1} = g \cdot k$, and then form the smash product $K * G$ corresponding to K, G, and f. This will not necessarily be a division algebra over F, but it will be a finite-dimensional central simple algebra, and as such isomorphic to a matrix ring $M_s(D)$ over some central division algebra D over F.

Now recall from the lecture on October 14 that there is an equivalence relation among central simple algebras over F such that equivalence classes form a group under the tensor product. The equivalence relation is that any two matrix rings $M_r(D), M_s(D)$ over the same division ring D are identified. The multiplicative inverse of an algebra A is the opposite algebra A^o defined on January 31 (in which the multiplication in A is reversed). Thus equivalence classes of central simple algebras over F form an abelian group, called the Brauer group of F and denoted $\mathrm{Br}(F)$ (see p. 830; I defined this toward the end of the lecture on October 14). With some work it can be shown that the product of two factor sets of a fixed extension K of F with Galois group G corresponds to the tensor product of the corresponding central simple algebras. Thus for fixed K and G, the second cohomology group $H^2(G, K^*)$ is a subgroup of $\mathrm{Br}(F)$. More precisely, the central simple algebras A such that $A \otimes_F K$ is a matrix ring over K are exactly those captured by $H^2(G, K^*)$.

I observed back in October that if F is algebraically closed then it is the only finite extension of itself, whence (up to equivalence) it is also the only central simple algebra over itself. Thus $\mathrm{Br}(F)$ is trivial for any such F. If $F = \mathbb{R}$, then I showed using the Sylow Theorems (and the Intermediate Value Theorem from analysis) that the only finite extensions of F are F and $\mathbb{C}$, the latter having Galois group $\mathbb{Z}_2$ over F. Since this is a cyclic group, it is a simple matter to compute its second cohomology group, and we find that the order of $\mathrm{Br}(\mathbb{R})$ is 2, as mentioned in October. The only central simple division algebras over $\mathbb{R}$ are $\mathbb{R}$ and the quaternion ring $\mathbb{H}$. Note that this shows that the *second* cohomology group of a Galois group, unlike the first one, need not be trivial. There are a few other examples of fields with trivial Brauer groups (e.g. fields of transcendence degree 1 over algebraically closed fields). It is known however that if the algebraic closure of a field is a finite extension, then that extension is either trivial or quadratic and can in fact be taken to be the extension by a square root of -1.

Looking at an opposite extreme, if instead F is finite, then you have proved in homework that all finite division rings are fields (Wedderburn's Theorem). Since all finite extensions of F are Galois with cyclic Galois group, it is not difficult to check directly that $H^2(\mathbb{Z}_n, K^*) = 0$, where $K = F_{q^n}$ is the finite field of order q^n, regarded as a Galois extension of F_q. In this way you get an alternate proof of Wedderburn's Theorem.

In general, though, a given field F admits many finite Galois extensions, with a wide variety of Galois groups. For example, I have mentioned that any finite group is the Galois group of an extension of the rational function field $\mathbb{C}(x)$ and it is widely believed that the same is true of $\mathbb{Q}$. To try to get some understanding of all central simple algebras over F at once, it is helpful to use something called inverse limits (see pp. 268,9). Given a group G, look at the collection $\{N_i : i \in I\}$ of its normal subgroups N_i. Partially order the index set I by reverse inclusion, so that $i \leq j$ if and only if $N_i \supseteq N_j$. Given any two normal subgroups N_i, N_j, their intersection $N_k = N_i \cap N_j$ is also normal and we have $i, j \leq k$. Any partially ordered set I with this last property is called a directed system (see p. 268).

Given the N_i as above, let $G_i = G/N_i$. Whenever $i \leq j$ we have a natural surjection $f_{ij} : G_j \to G_i$ given by the projection map; if $i \leq j \leq k$ then the composition $f_{jk} \circ f_{ij} = f_{ik}$. In general, suppose that we are given a directed system I, a family of groups $\{G_i\}$ indexed by I, and for each $i, j \in I$ with $i \leq j$ a group homomorphism $f_{ij} : G_j \to G_i$ such that $f_{ii} = 1$ for all i and if $i \leq j \leq k$, then $f_{ik} = f_{jk} \circ f_{ij}$. Then we can form the set $\overleftarrow{G}$ of I-tuples $\{g_i : i \in I\}$ such that $g_i \in G_i$ and $f_{ij}(g_j) = g_i$ for $i \leq j$. This is a group under multiplication, called the inverse limit of the G_i. In the special case $G_i = G/N_i$ with the N_i as above there is a natural map $G \to \overleftarrow{G}$ sending g to the I-tuple with g_i equal to the image of g in G_i for all i. The kernel of the map is the intersection of the N_i. A group that is the inverse limit of finite groups is called profinite (p. 809).

The application to central simple algebras over F arises when we let L be the algebraic closure of F and take G to be the (full) Galois group of L over F. The Galois group G of L over F may then be identified with the profinite direct limit of the Galois groups of the finite Galois extensions of F (each lying in L). The second cohomology group of this group is then isomorphic to the Brauer group of F.

In the meantime, a small personal note: like you I first learned about central simple algebras in my first year of graduate school. I paid no particular attention to them at the time but a few years later realized that that the cohomology groups used to construct them would play a central role in my thesis; fortunately I had saved both my notes from that year and the text that was used then. A lesson that one must never throw anything away!

Specifically, the group cohomology that I cited in my thesis was the Schur multiplier, defined to be the group $H^2(G, \mathbb{C}^*)$, where G is a finite group acting trivially on the multiplicative group $\mathbb{C}^*$ of complex numbers. This group is trivial if G is cyclic, but not in general even for noncyclic abelian groups. Its nontriviality enabled me to disprove a conjecture my advisor had made.