Lecture 5-1: Factor sets, group extensions, and H^2

May 1, 2024

Having studied split extensions of G by A in detail, we turn attention now to (possibly nonsplit) extensions. We will see that these are controlled by the next higher cohomology group $H^2(G, A)$ and derive a condition under which all of them are split. We will then work out an example in detail.

Given an extension $1 \to A \to E \to G \to 1$ with A abelian, note first that E acts on A by conjugation and the restriction of this action to A is trivial, so that $G \cong E/A$ also acts on A. It is easy to check that equivalent extensions $1 \to A \to E \to G \to 1$ and $1 \to A \to E' \to G \to 1$ induce the same action of G on A, so we can assume that the action of G on A has been fixed and consider only extensions inducing this action.

Given such an extension, for each $g \in G$ choose a representative e_g of the right coset Ag of A in E. Then for $g, h \in G$ we must have $e_g e_h = a_{g,h} e_{gh}$ for some $a_{g,h} \in A$. If $k \in G$, then the associative law forces $(e_g e_h)e_k = e_g(e_h e_k)$, whence $a_{g,h} e_{gh} e_k = a_{g,h} a_{gh,k} e_{ghk} = e_g(e_h e_k) = e_g(a_{h,k} e_{hk}) = (g a_{h,k}) a_{g,hk} e_{ghk}$. Cancelling e_{ghk} and reverting to additive notation for A we get $a_{g,h} + a_{gh,k} = g a_{h,k} + a_{g,hk}$. Rewriting $a_{g,h}$ as $f(g,h)$ (and calling it a factor set), this last condition is exactly the one for f to lie in $Z^2(G, A)$. Moreover, if we choose another representative $e'_g = \alpha_g e_g$ of the same coset Ag for all $g \in G$, so that $\alpha_g \in A$, and write $e'_g e'_h = a'_{g,h} e'_{gh}$, then we find that $a'_{g,h} = a_{g,h} + \alpha_g + g\alpha(h) - \alpha_{gh}$, so that $a_{g,h}$ and $a'_{g,h}$ differ by a 1-coboundary. As it is easy to check that two extensions are equivalent if and only if their factor sets are related in this way, we get

Theorem 36, DF, p. 828

For a fixed action of G on A, equivalence classes of extensions inducing this action are in bijection to cohomology classes in $H^2(G, A)$. The split extension (with E the semidirect product of A and G) corresponds to the trivial cohomology class.

We can simplify the analysis of factor sets f by choosing the identity element $e_1 = 1$ to represent the identity coset $A1$; then $f(1, g) = f(g, 1) = 0$ for all $g \in G$. Factor sets satisfying this condition are called normalized; every factor set lies in the same cohomology class as a normalized one.

Corollary: DF, p. 828

If A is finite and its order is relatively prime to that of G, then every extension of G by A splits. Any two complements of A in an extension E are conjugate under A.

This follows since once again a previous result guarantees that $H^1(G, A) = H^2(G, A) = 0$ in this situation.

Once this result is known, some simple group theory extends it to the case where A is not abelian.

Schur's Theorem, DF, p. 829

If E is a finite group containing a normal subgroup N whose order and index are relatively prime, then N has a complementary subgroup H in E, so that E is a split extension of H by N.

Proof.

By induction on the order of E. Since we may assume that $N \neq 1$, let p be a prime dividing the order $|N|$ of N and let P be a Sylow p-subgroup of N, with normalizer E_0 in E. Set $N_0 = N \cap E_0$. Since any conjugate ePe^{-1} of P is p-Sylow in N and thus conjugate in N to P, we have $E = E_0N$, whence N_0 is normal in E_0 and the index $[E_0 : N_0]$ of N_0 in E_0 equals the index $[E : N]$ of N in E. If $E_0 \neq E$, then by inductive hypothesis N_0 has a complement H in E_0, which is also a complement to N in E, as desired. Hence we may assume $E_0 = E$, so that P is normal in E. The center $Z(P)$ of P, like P itself, is then preserved by conjugation in E, so is normal. □

Proof.

If $Z(P) = N$ then N is abelian and we are done by the previous corollary. Otherwise we pass to the quotient group $\overline{E} = E/Z(P)$. The image $\overline{N}$ of N in this group has index relatively prime to its order, so that group has a complement $\overline{H}$ in $\bar{E}$. The preimage E_1 of $\overline{H}$ in E then has $|E_1| = |\overline{H}||Z(P)| = |E/N||Z(P)|$, so $Z(P)$ has relatively prime order and index in E_1. By induction it has a complement H in E_1 which by its order must be a complement to N in E, as desired. □

As an example, take E to be the alternating group A_4. This group has K, the Klein four-group, as a normal subgroup whose index 3 is relatively prime to 4, so it has a complementary subgroup. Up to conjugacy, the unique such subgroup is T, the cyclic group generated by a 3-cycle, say (123), in E. Conversely, the subgroup T is such that $gTg^{-1} \cap T = 1$ for $g \notin T$, so by Frobenius's Theorem (proved by induced characters), T is a complement of a normal subgroup of E. Of course this unique normal subgroup is just K.

Another example, to which I have a small personal connection, is the *Schur multiplier* of a finite group G, which is by definition the cohomology group $H^2(G, \mathbb{C}^*)$, where the action of G on $\mathbb{C}^*$ is trivial. Like all of you, I first learned about factor sets and group cohomology in a first-year algebra course. Although I paid no particular attention to this material when I first learned it, I realized a few years later that the Schur multiplier was going to play a crucial role in my thesis. Fortunately, I still had both my old book and notes on group cohomology; this is a lesson that one must never throw anything away!

We conclude with an extended example, following the discussion on pp. 830,1 in DF. Take G to be the Klein four-group and write its elements as $1, a, b, c$. Take A to be the cyclic group of order 2, on which G (necessarily) acts trivially. To compute the group $H^2(G, A)$ we must first look at groups E admitting a normal cyclic subgroup of order 2 (necessarily central) such that the quotient of E by this subgroup is isomorphic to G. The possibilities for E are $(\mathbb{Z}/2\mathbb{Z})^3$, the quaternion group Q (of order 8), the product $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the dihedral group D of order 8. There is only one extension up to equivalence in the first and last cases, since the automorphisms of E necessarily fix A and induce the full set of automorphisms of G.

The other two cases offer more possibilities. If E is the direct product of cyclic subgroups $\langle x \rangle, \langle y \rangle$ of orders 4 and 2, respectively, then we must take A to be the subgroup generated by x^2. An automorphism of E must send x to one of x, x^3, xy, x^3y, while y goes to itself or to x^2y. Modulo x^2, then y must go to itself and there are just tow choices for the image of x, so that only two of the six automorphisms of G arise from automorphisms of E. Accordingly, there are three inequivalent extensions with this group E. Similarly, if $E \cong D$ is generated by the cyclic subgroups $\langle r \rangle$ and $\langle s \rangle$ of orders 4 and 2 generated by a rotation r and a reflection s, respectively, then we must have $A = \langle r^2 \rangle$. An automorphism of E sends r to itself or r^3, so that modulo A, r must go to itself, and again only two of the six automorphisms of G arise from automorphisms of E. Thus there are again three inequivalent extensions with this group E.

As every nonidentity element of $H^2(G, A)$ has order 2, we must have $H^2(G, A) \cong (\mathbb{Z}/2\mathbb{Z})^3$. Actually, there is more structure present here, which can be used to better explain what is going on. If A and B are two G-modules, then it is easy to see that $H^n(G, A \oplus B)$ is the direct sum of $H^n(G, A)$ and $H^n(G, B)$ for all n. But if instead G, H are two groups equipped with commuting actions on A, then $H^n(G \times H, A)$ is *not* the direct sum of $H^n(G, A)$ and $H^n(H, A)$. Just to leave you in suspense, I will defer explaining this until next time.