Lecture 2-10 H^2 and group extensions

February 10, 2025

Let $H = A \ltimes G$ be a semidirect product of finite groups with the normal subgroup A ablelian. Toward the end of last time, I showed that A-conjugacy classes of subgroups G' of H mapping isomorphically onto G by the projection $\pi : H \to G$ are parametrized by the first cohomology group $H^1(G, A)$. Such groups H are called (split) extensions of G by A. A natural follow-up to this would be to look at extensions that are not necessarily split, that is, groups E with A as a normal subgroup such that $E/A \cong G$ but where E does not necessarily have a subgroup isomorphic to G. This lecture is devoted to studying such extensions.

More formally, one has

Definition, p. 824

An *extension* of a group G by an abelian group A is a short exact sequence $1 \to A \to E \to G \to 1$ of groups such that A (or rather its image in E is normal. Two extensions $1 \to A \to E \to G \to 1, 1 \to A \to E' \to G \to 1$ are *equivalent* if there is a group isomorphism $\beta : E \to E'$ such that the obvious diagram with rows the short exact sequences and column maps given by the identity, β, and the identity, commutes.

I emphasize that for two extensions with middle terms E, E' to be equivalent it is *not* sufficient that E and E' be isomorphic. Last quarter we looked at extensions $0 \to L \to M \to N \to 0$ of modules over a ring R; in this setting L is automatically a normal subgroup of M as an abelian group. In that setting also for two extensions with middle terms M, M' to be equivalent it is not sufficient that M and M' be isomorphic.

Given an extension of G by A with middle term E, for each $g \in G$ choose $\mu(g)_{\in} E$ mapping onto g by the surjection $E \to G$. Then for $g, h \in G$ the product $\mu(g)\mu(h) = f(g, h)\mu(g, h)$ for some $f :\in C^2(G, A)$. We call f a factor set (p. 825). Taking $\mu(1) = 1$, we can arrange that $f(1, g) = f(g, 1) = 0$, the identity element of A (using additive notation); if this holds we say that the factor set f is normalized. The associative law for the product $\mu(g)\mu(h)\mu(k)$ then shows that

$$f(g, h) + f(gh, k) = g \cdot f(h, k) + f(g, hk);$$

again in additive notation; this is sometimes called the factor set condition. This is exactly the condition for f to be a 2-cocycle, by the bar resoslution. If we make a different choice of μ, replacing $\mu(g)$ by $f_1(g)\mu(g)$ for some $f_1 \in C(G, A)$, then the factor set f gets replaced by f', where $f'(g, h) = f(g, h) + g \cdot f_1(h) - f_1(gh) + f_1(g)$; this is exactly the condition that f and f' differ by a 1-coboundary.

Conversely, suppose we have a group G acting on an abelian group A by automorphisms. Let $f : G^2 \to A$ be a 2-cocycle. Define a formal symbol $\mu(g)$ for $g \in G$, impose the relation $\mu(g)\mu(h) = f(g, h)\mu(g, h)$ for $g, h \in G$ and decree that μ_g act on A by conjugation as g does. Then A and the μ_g generate a group E and an extension $1 \to A \to E \to G \to 1$; the map from E to G has kernel A and sends each $\mu(g)$ to g.

I deduce

Theorem 36, p. 828

There is a 1-1 correspondence between equivalence classes of extensions of G by A and elements of $H^2(G, A)$. The zero element of $H^2(G, A)$ corresponds to the class of split extensions.

I showed last time that $H^n(G, A) = 0$ for all $n \geq 0$ if A and G are finite with relatively prime orders. Now I get (using the last result last time)

Schur's Theorem, p. 829

If a finite group E has an abelian normal subgroup A whose index is relatively prime to its order, then E is the semidirect product of A and a complementary subgroup G. Moreover any two complements of A in E are conjugate under A.

Returning to the two examples of Frobenius groups that I gave last quarter, I note that the symmetric group S_3 has the normal abelian subgroup A_3 whose order and index are relatively prime; here the three subgroups generated by transpositions are conjugate and complementary to A_3. Similarly, the alternating group A_4 has the Klein 4-group K as a normal abelian subgroup, whose index is relatively prime to its order. Here there are four complements of K in A_4, each generated by a 3-cycle. Note that while it is not true that any two 3-cycles are conjugate in A_4, it is true that any two *subgroups* generated by 3-cycles are conjugate; in fact such subgroups are exactly 3-Sylow subgroups of A_4.

Once one knows Schur's Theorem for abelian normal subgroups, it turns out that purely group-theoretic arguments establish it for general normal subgroups.

Schur's Theorem in general, p. 829

If a finite group E has a normal subgroup whose order and index are relatively prime, then E is the semidirect product of N and a complementary subgroup G.

Proof.

By induction on the order of E. Since we may assume that $N \neq 1$, let p be a prime dividing the order of N and let P be a p-Sylow subgroup of N, with normalizer E_0 in E. Set $N_0 = N \cap E_0$. Since any conjugate ePe^{-1} for $e \in E$ is p-Sylow in N and thus conjugate in N to P, we have $E = E_0 N$, whence N_0 is normal in E_0 and the index $[E_0 : N_0] = [E : N]$. 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 that $E_0 = E$, so that P is normal in E. The center Z of P, like P itself, is then preserved by conjugation in E, so is normal. □

Proof.

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

I do not know whether any two complements of N in E must be conjugate by N in the general setting. Following the text (pp. 830-31), I now present the simplest example of a noncyclic group not satisfying the hypothesis of Schur's Theorem, so that its cohomology (with suitable coefficients) is nonzero. Take G to be $\mathbb{Z}_2 \times \mathbb{Z}_2$, 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. Here the order and index of A in an extension of G by A are not relatively prime. The possibilities for a group E admitting a normal (necessarily central) cyclic subgroup A of order 2 such that $E/A \cong G$ are $\mathbb{Z}_2^3$, the quaternion group H, the product $\mathbb{Z}_4 \times \mathbb{Z}_2$, 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 all possible automorphisms of G.

The other two cases offer more possibilities. If E is the product of cyclic groups of orders 4 and 2, generated respectively by x and y, then we may take A to be the subgroup generated by x^2. An automorphism of E must send x to one of x, x^3, xy, and x^3y, while y goes to itself or to x^2y. Modulo x^2, then, y must go to itself and there are just two choices for the image of x, so only two of the six automorphisms of G arise from automorphisms of E and there are three inequivalent extensions with this group E. Similarly, taking $E = D$, generated by the cyclic subgroups $\langle r \rangle, \langle s \rangle$ generated by a rotation and reflection, respectively, then we must take $A = \langle r^2 \rangle$. Automorphisms of E must send r to itself or its inverse, so again the induced automorphisms of E/A send the image of r to itself and offer just two choices for the image of s. Again only two of the six automorphisms of G arise from automorphisms of E and we get three inequivalent extensions for this E.

Thus there are eight inequivalent extensions of G by A altogether. Since every element of $H^2(G, A)$ has order 2, we must have $H^2(G, A) \cong \mathbb{Z}_2^3$ as an abelian group. Actually, there is more structure present here, with which those of you with a background in algebraic topology might be familiar. The direct sum $R = \oplus_n H^n(G, A)$ of all the cohomology groups attached to G and A has a ring structure, given by something called the cup product, and the ring R is then graded, since the product of classes in $H^n(G, A)$ and $H^m(G, A)$ turns out to land in $H^{n+m}(G, A)$, From this point of view, the cohomology ring $R' = \oplus_n H^n(\mathbb{Z}_2, A)$ turns out to be the polynomial ring $\mathbb{Z}_2[x]$.

In general, given a direct product $G_1 \times G_2$ of groups acting trivially on a field k, something called the Künneth formula asserts that the cohomology ring attached to $(G_1 \times G_2, A)$ is the tensor product over k of the rings attached to (G_1, A) and (G_2, A). In the present case, with $k = \mathbb{Z}_2$, taking the tensor product of the polynomial rings $\mathbb{Z}_2[x]$ and $\mathbb{Z}_2[y]$, we get the polynomial $\mathbb{Z}_2[x, y]$ in two variables, graded by total degree. The 2-graded piece is spanned by x^2, xy, and y^2: these monomials form a basis of the three-dimensional space $H^2(G, \mathbb{Z}_2)$ over $\mathbb{Z}_2$.