where $m(a)$ is the number of elements among $a, 2a, \ldots, (p-1)a/2$ whose least positive remainder modulo p is greater than $(p-1)/2$ (in which case the element differs by -1 from one of our chosen coset representatives and contributes one factor of -1 to the product in (24)). This result is known as *Gauss' Lemma* in elementary number theory and can be used to prove Gauss' celebrated Quadratic Reciprocity Law (cf. also Exercise 15).

Next we give two important interpretations of $H^1(G, A)$ in terms of semidirect products. If A is a G-module, let E be the semidirect product $E = A \rtimes G$, where A is normal in E and the action of G (viewed as a subgroup of E) on A by conjugation is the same as its G-module action: $gag^{-1} = g \cdot a$. In the notation of Section 5.5, $E = A \rtimes_\varphi G$, where φ is the homomorphism of G into $\mathrm{Aut}(A)$ given by the G-module action. In particular, E will be the direct product of A and G if and only if G acts trivially on A. As in Section 5.5, we shall write the elements of E as (a, g) where $a \in A$ and $g \in G$, with group operation

$$(a_1, g_1)(a_2, g_2) = (a_1 + g_1 \cdot a_2, g_1 g_2).$$

Note that A is written additively, while G and E are written multiplicatively.

Definition. Let X be any group and let Y be a normal subgroup of X. The *stability group* of the series $1 \trianglelefteq Y \trianglelefteq X$ is the group of all automorphisms of X that map Y to itself and act as the identity on both of the factors Y and X/Y, i.e.,

$$\mathrm{Stab}(1 \trianglelefteq Y \trianglelefteq X) = \{\sigma \in \mathrm{Aut}(X) \mid \sigma(y) = y \text{ for all } y \in Y, \text{ and } \sigma(x) \equiv x \bmod Y \text{ for all } x \in X\}.$$

In the special case where Y is an *abelian* normal subgroup of X, conjugation by elements of Y induce (inner) automorphisms of X that stabilize the series $1 \trianglelefteq Y \trianglelefteq X$, and in this case $Y/C_Y(X)$ is isomorphic to a subgroup of $\mathrm{Stab}(1 \trianglelefteq Y \trianglelefteq X)$ (where $C_Y(X)$ is the elements of Y in the center of X).

Proposition 31. Let A be a G-module and let E be the semidirect product $A \rtimes G$. For each cocycle $f \in Z^1(G, A)$ define $\sigma_f : E \to E$ by

$$\sigma_f((a, g)) = (a + f(g), g).$$

Then the map $f \to \sigma_f$ is a group isomorphism from $Z^1(G, A)$ onto $\mathrm{Stab}(1 \trianglelefteq A \trianglelefteq E)$. Under this isomorphism the subgroup $B^1(G, A)$ of coboundaries maps onto the subgroup $A/C_A(E)$ of the stability group.

Proof: It is an exercise to see that the cocycle condition implies σ_f is an automorphism of E that stabilizes the chain $1 \trianglelefteq A \trianglelefteq E$. Likewise one checks directly that $\sigma_{f_1+f_2} = \sigma_{f_1} \circ \sigma_{f_2}$, so the map $f \mapsto \sigma_f$ is a group homomorphism. By definition of σ_f this map is injective. Conversely, let $\sigma \in \mathrm{Stab}(1 \trianglelefteq A \trianglelefteq E)$. Since σ acts trivially on E/A, each element $(0, g)$ in this semidirect product maps under σ to another element (a, g) in the same coset of A; define $f_\sigma : G \to A$ by letting $f_\sigma(g) = a$. If we identify A with the elements of the form $(a, 1)$ in E, then the group operation in E shows that

$$f_\sigma(g) = \sigma((0, g))(0, g)^{-1}.$$

Because σ is a stability automorphism of E, it is easy to check that f_σ satisfies the cocycle condition. It follows immediately from the definitions that $f_{\sigma_f} = f$, so the map $f \mapsto \sigma_f$ is an isomorphism.

Now f is a coboundary if and only if there is some $x \in A$ such that $f(g) = x - g \cdot x$ for all $g \in G$. Thus f is a coboundary if and only if $\sigma_f((a, g)) = (a + x - g \cdot x, g)$. But conjugation in E by the element $(x, 1)$ maps (a, g) to the same element $(a + x - g \cdot x, g)$, so the automorphism σ_f is conjugation by $(x, 1)$. This proves the remaining assertion of the proposition.

Corollary 32. In the notation of Proposition 31 let φ_a denote the automorphism of E given by conjugation by a for any $a \in A$. Then the cocycles f_1 and f_2 are in the same cohomology class in $H^1(G, A)$ if and only if $\sigma_{f_1} = \varphi_a \circ \sigma_{f_2}$, for some $a \in A$.

The proposition and corollary show that 1-cocycles may be computed by finding automorphisms of E that stabilize the series $1 \trianglelefteq A \trianglelefteq E$, and vice versa. The first cohomology group is then given by taking these automorphisms modulo inner automorphisms, i.e., is the group of "outer stability automorphisms" of this series.

Example

Let $G = Z_2$ act by inversion on $A = \mathbb{Z}/4\mathbb{Z}$. The corresponding semidirect product $E = A \rtimes G$ is the dihedral group of order 8, which has automorphism group isomorphic to D_8; viewing E as a normal (index 2) subgroup of D_{16}, conjugation in the latter group restricted to E exhibits 8 distinct automorphisms of E (cf. Proposition 17 in Section 4.4). The subgroup A of E is characteristic in E, hence every automorphism of E sends A to itself, and therefore also acts on E/A (necessarily trivially since $|E/A| = 2$). Half the automorphisms of E invert A and half centralize A; in fact, the cyclic subgroup of order 8 in D_{16} (which contains A) maps to a cyclic group of order 4 of automorphisms centralizing A. Thus $\mathrm{Stab}(1 \trianglelefteq A \trianglelefteq E) \cong Z_4 \cong Z^1(G, A)$. Since the center of E is a subgroup of A of order 2, $|A/Z(E)| = 2 = |B^1(G, A)|$. This proves $|H^1(G, A)| = 2$.

In the semidirect product E the subgroup G is a complement to A, i.e., $E = AG$ and $A \cap G = 1$; moreover, every E-conjugate of G is also a complement to A. But A may have complements in E that are not conjugate to G in E. Our second interpretation of $H^1(G, A)$ shows that this cohomology group characterizes the E-conjugacy classes of complements of A in E.

Proposition 33. Let A be a G-module and let E be the semidirect product $A \rtimes G$. For each 1-cocycle f let

$$G_f = \{(f(g), g) \mid g \in G\}.$$

Then G_f is a subgroup complement to A in E. The map $f \mapsto G_f$ is a bijection from $Z^1(G, A)$ to the set of complements to A in E. Two complements are conjugate in E if and only if their corresponding 1-cocycles are in the same cohomology class in $H^1(G, A)$, so there is a bijection between $H^1(G, A)$ and the set of E-conjugacy classes of complements to A.

Proof: By the cocycle condition,

$$(f(g), g)(f(h), h) = (f(g) + gf(h)g^{-1}, gh) = (f(g) + g \cdot f(h), gh) = (f(gh), gh),$$

and it follows that G_f is closed under the group operation in E. As observed earlier, each cocycle necessarily has $f(1) = 0$, so G_f contains the identity $(0, 1)$ of E. The inverse to $(f(g), g)$ in E is $(f(g^{-1}), g^{-1})$, so G_f is closed under inverses. This proves G_f is a subgroup of E. Since the distinct elements of G_f represent the distinct cosets of A in E, G_f is a complement to A in E. Distinct cocycles give different coset representatives, hence they determine different complements.

Conversely, if C is any complement to A in G, then C contains a unique coset representative $a_g g$ of Ag for each $g \in G$. Since C is closed under the group operation the element $(a_g g)(a_h h) = (a_g g a_h g^{-1})gh$ represents the coset Agh, and so a_{gh} is $a_g g a_h g^{-1} = a_g(g \cdot a_h)$ (written additively in A this becomes $a_{gh} = a_g + (g \cdot a_h)$). This shows that the map $f : G \to A$ given by $f(g) = a_g$ is a cocycle, and so $C = G_f$. Hence there is a bijection between 1-cocycles and complements to A in E.

Since $\mathrm{Stab}(1 \trianglelefteq A \trianglelefteq E)$ normalizes A it permutes the complements to A in E. In the notation of Proposition 31, for 1-cocycles f_1 and f_2 it follows immediately from the definition that $\sigma_{f_1}(G_{f_2}) = G_{f_1+f_2}$. This shows that the permutation action of $\mathrm{Stab}(1 \trianglelefteq A \trianglelefteq E)$ on the set of complements to A in E is the (left) regular representation of this group. Furthermore, if $a \in A$ and φ_a is the stability automorphism conjugation by a, then

$$aG_f a^{-1} = \varphi_a(G_f) = G_{f+\beta_a} \tag{17.25}$$

where β_a is the 1-coboundary $\beta_a : g \mapsto a - g \cdot a$. Since G_f is a complement to A, any $e \in E$ may be written as ag for some $a \in A$ and $g \in G_f$. Then $eG_f e^{-1} = aG_f a^{-1}$, i.e., the E-conjugates of G_f are the just the A-conjugates of G_f. Now the complements G_{f_1} and G_{f_2} are conjugate in E if and only if $G_{f_2} = aG_{f_1}a^{-1} = G_{f_1+\beta_a}$ for some $a \in A$ by (25). This shows two complements are conjugate in E if and only if their corresponding cocycles differ by a coboundary, i.e., represent the same cohomology class in $H^1(G, A)$, which completes the proof.

Corollary 34. Under the notation of Proposition 33, all complements to A are conjugate in E if and only if $H^1(G, A) = 0$.

Corollary 35. If A is a finite abelian group whose order is relatively prime to $|G|$ then all complements to A in any semidirect product $E = A \rtimes G$ are conjugate in E.

Examples

(1) Let $A = \langle a \rangle$ and $G = \langle g \rangle$ both be cyclic of order 2. The group G must act trivially on A, hence $A \rtimes G = A \times G$ is a Klein 4-group. Here $A \rtimes G$ is abelian, so every subgroup is conjugate only to itself, and since $H^1(G, A) = \mathrm{Hom}(Z_2, \mathbb{Z}/2\mathbb{Z})$ has order 2, there are precisely two complements to A in E, namely $\langle g \rangle$ and $\langle ag \rangle$.

(2) If $A = \langle a \rangle$ is cyclic of order 2 and $G = \langle x \rangle \times \langle y \rangle$ is a Klein 4-group, then as before G must act trivially on A, so $H^1(G, A) = \mathrm{Hom}(Z_2 \times Z_2, \mathbb{Z}/2\mathbb{Z})$ has order 4. The four complements to A in $A \times G$ are G, $\langle ax, y \rangle$, $\langle x, ay \rangle$ and $\langle ax, ay \rangle$.

(3) Proposition 33 can also be used to compute $H^1(G, A)$. Let $A = \langle r \rangle$ be cyclic of order 4 and let $G = \langle s \rangle$ be cyclic of order 2 acting on A by inversion: $srs^{-1} = r^{-1}$ as in the Example following Corollary 32. Then $A \rtimes G$ is the dihedral group D_8 of order 8. The subgroup A has four complements in D_8, namely the groups generated