As a special case, suppose K/F is a Galois extension with cyclic Galois group G having generator σ. The cohomology groups for G were computed explicitly in the previous section, and in particular, $H^1(G, A) = {}_N A/(\sigma - 1)A$ for any G-module A (written additively). Since this group is trivial in the present context, we see that an element α in K is in the kernel of the norm map, i.e., $\mathrm{N}_{K/F}(\alpha) = 1$ if and only if $\alpha = \sigma(\beta)/\beta$ for some $\beta \in K$. (For a direct proof of this result in the cyclic case, cf. Exercise 23 in Section 14.2.)

This famous result for cyclic extensions was first proved by Hilbert and appears as "Theorem 90" in his book (known as the "*Zahlbericht*") on number theory in 1897. As a result, the more general result $H^1(G, K^\times) = 0$ is referred to in the literature as "Hilbert's Theorem 90." In general, the higher dimensional cohomology groups $H^n(G, K^\times)$ for $n \geq 2$ can be nontrivial (cf. Exercise 13).

Example

Suppose $G = \mathrm{Gal}(K/F)$ is the Galois group of a finite Galois extension K/F of fields as in the previous example. Then the additive group K is also a G-module and $H^n(G, K) = 0$ for all $n \geq 2$. The proof of this in general uses the fact that there is a *normal basis* for K over F, i.e., there is an element $\alpha \in K$ whose Galois conjugates give a basis for K as a vector space over F, or, equivalently, $K \cong \mathbb{Z}G \otimes_{\mathbb{Z}} F$ as G-modules. The latter isomorphism shows that K is induced as a G-module, and then $H^n(G, K) = 0$ follows from Corollary 24 in Section 2. For a direct proof in the case where G is cyclic, cf. Exercise 26 in Section 14.2.

If G acts trivially on A, then $g \cdot a - a = 0$, so 0 is the only principal crossed homomorphism, i.e., $B^1(G, A) = 0$. This proves the following result:

Proposition 30. If A is a G-module on which G acts trivially then $H^1(G, A) = \mathrm{Hom}(G, A)$, the group of all group homomorphisms from G to H.

If G is a profinite group, then the same result holds for the continuous cohomology group $H^1(G, A)$ provided one takes the group of continuous homomorphisms from G into A.

Examples

(1) If G acts trivially on A then $H^1(G, A) = H^1(G/[G, G], A)$ since any group homomorphism from G to the abelian group A factors through the commutator subgroup $[G, G]$ (cf. Proposition 7(5) in Section 5.4), so computing H^1 for trivial G-action reduces to computing H^1 for some abelian group.

(2) If G is a finite group acting trivially on $\mathbb{Z}$, then $H^1(G, \mathbb{Z}) = 0$ because $\mathbb{Z}$ has no nonzero elements of finite order so there is no nonzero group homomorphism from G to $\mathbb{Z}$.

(3) If A is cyclic of prime order p and G is a p-group then G must act trivially on A (since the automorphism group of A has order $p - 1$), so in this case one always has $H^1(G, A) = \mathrm{Hom}(G, A)$.

(4) If G is a finite group that acts trivially on $\mathbb{Q}/\mathbb{Z}$ then $H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \hat{G}$ is the *dual group* of G (cf. Exercise 14 in Section 5.2.). Since $\mathbb{Q}/\mathbb{Z}$ is abelian, any homomorphism of G into $\mathbb{Q}/\mathbb{Z}$ factors through the commutator quotient $G^{\mathrm{ab}} = G/[G, G]$ of G, so $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z})$. It follows that $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \widehat{G^{\mathrm{ab}}}$ (which by cf. Exercise 14 again is noncanonically isomorphic to G^{ab}).

If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules then the long exact sequence in group cohomology in Theorem 21 of the previous section begins with terms

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta_0} H^1(G, A) \longrightarrow \cdots.$$

The connecting homomorphism δ_0 is given explicitly as follows: if $c \in C^G$ then there is an element $b \in B$ mapping to c and then $\delta_0(c)$ is the class in $H^1(G, A)$ of the 1-cocycle given by

$$\begin{aligned} \delta_0(c) : G &\longrightarrow A \\ g &\longmapsto g \cdot b - b. \end{aligned}$$

Note that $g \cdot b - b$ is (the image in B of) an element of A for all $g \in G$ since $c \in C^G$. To verify directly that $f = \delta_0(c)$ satisfies the cocycle condition in (20), we compute

$$f(gh) = gh \cdot b - b = (g \cdot b - b) + g \cdot (h \cdot b - b) = f(g) + gf(h).$$

From the explicit expression $f = g \cdot b - b$ it is also clear that $\delta_0(c) \in H^1(G, A)$ maps to 0 in the next term $H^1(G, B)$ of the long exact sequence above since f is the coboundary for the element $b \in B$.

Example: (Kummer Theory)

Suppose that F is a field of characteristic 0 containing the group μ_n of all n^{th} roots of unity for some $n \geq 1$. Let K be an algebraic closure of F and let $G = \text{Gal}(K/F)$. The group G acts trivially on μ_n since $\mu_n \subset F$ by assumption, i.e., $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ as G-modules. Hence the Galois cohomology group $H^1(G, \mu_n)$ is the group $\text{Hom}_c(G, \mathbb{Z}/n\mathbb{Z})$ of continuous homomorphisms of G into $\mathbb{Z}/n\mathbb{Z}$. If χ is such a continuous homomorphism, then $\ker \chi \subseteq G$ is a closed normal subgroup of G, hence corresponds by Galois theory to a Galois extension L_χ/F. Then $\text{Gal}(L_\chi/F) \cong \text{image}\ \chi$, so L_χ is a cyclic extension of F of degree dividing n. Conversely, every such cyclic extension of F defines an element in $\text{Hom}_c(G, \mathbb{Z}/n\mathbb{Z})$, so there is a bijection between the elements of the Galois cohomology group $H^1(G, \mu_n)$ and the cyclic extensions of F of degree dividing n.

The homomorphism of raising to the n^{th} power is surjective on $K^\times$ (since we can always extract n^{th} roots in K) and has kernel μ_n. Hence the sequence

$$1 \longrightarrow \mu_n \longrightarrow K^\times \xrightarrow{n} K^\times \longrightarrow 1$$

is an exact sequence of discrete G-modules. The associated long exact sequence in Galois cohomology gives

$$1 \longrightarrow \mu_n^G \longrightarrow (K^\times)^G \xrightarrow{n} (K^\times)^G \longrightarrow H^1(G, \mu_n) \longrightarrow H^1(G, K^\times) \longrightarrow \cdots.$$

We have $\mu_n^G = \mu_n$ and $(K^\times)^G = F^\times$ by Galois theory, and $H^1(G, K^\times) = 0$ by Hilbert's Theorem 90, so this exact sequence becomes

$$1 \longrightarrow \mu_n \longrightarrow F^\times \xrightarrow{n} F^\times \longrightarrow H^1(G, \mu_n) \longrightarrow 0,$$

which in turn is equivalent to the isomorphism

$$H^1(G, \mu_n) \cong F^\times/F^{\times^n}$$

where $F^{\times^n}$ denotes the group of n^{th} powers of elements of $F^\times$. This isomorphism is made explicit using the explicit form for the connecting homomorphism given above: for every $\alpha \in F^\times$ and $\sigma \in G$, the element $\sqrt[n]{\alpha}$ in $K^\times$ maps to α in the exact sequence and

$$\chi(\sigma) = \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}$$

defines an element in $H^1(G, \mu_n)$ (cf. Exercise 11). The kernel of this homomorphism χ is the field $F(\sqrt[n]{\alpha})$. By the results of the previous paragraph, when F contains the n^{th} roots of unity an extension L/F is Galois with cyclic Galois group of order dividing n if and only if $L = F(\sqrt[n]{\alpha})$ for some $\alpha \in F^\times$. Furthermore, the class of α in $F^\times/F^{\times^n}$ is unique, i.e., α is unique up to an n^{th} power of an element in F. Such an extension is called a *Kummer extension*, cf. Section 14.7 and Exercise 12.

If the characteristic of F is a prime p, the same argument applies when n is not divisible by p, replacing the algebraic closure of F with the separable closure of F (the largest separable algebraic extension of F).

Example: (The Transfer Homomorphism)

Suppose G is a finite group and H is a subgroup. The corestriction defines a homomorphism from $H^1(H, \mathbb{Q}/\mathbb{Z})$ to $H^1(G, \mathbb{Q}/\mathbb{Z})$, which by Example 4 above gives a homomorphism from $\widehat{H^{\text{ab}}}$ to $\widehat{G^{\text{ab}}}$. This gives a homomorphism

$$\text{Ver} : G^{\text{ab}} \longrightarrow H^{\text{ab}}$$

called the *transfer* (or *Verlagerungen*) homomorphism (cf. Exercise 14). To make this homomorphism explicit, consider the exact sequence

$$0 \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow M_1^G(\mathbb{Q}/\mathbb{Z}) \longrightarrow C \longrightarrow 0 \tag{17.22}$$

defined by the homomorphism mapping $a \in \mathbb{Q}/\mathbb{Z}$ to $f_a \in M_1^G(\mathbb{Q}/\mathbb{Z})$ in Example 4 preceding Proposition 23 in the previous section (so $f_a(g) = g \cdot a$ for $g \in G$). This is a short exact sequence of G-modules and hence also of H-modules. The first portions of the associated long exact sequences for the cohomology with respect to H and then G give the rows in the commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r] & C^H \arrow[r, "\delta_0"] \arrow[d, "\text{Cor}"] & H^1(H, \mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "\text{Cor}"] & 0 \\
\cdots \arrow[r] & C^G \arrow[r, "\delta_0"] & H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r] & 0
\end{tikzcd}$$

since $H^1(H, M_1^G(\mathbb{Q}/\mathbb{Z})) = H^1(G, M_1^G(\mathbb{Q}/\mathbb{Z})) = 0$ (cf. Exercise 12 in Section 2). Let $\chi \in H^1(H, \mathbb{Q}/\mathbb{Z})$ and suppose that $c \in C^H$ is an element mapping to χ by the surjective connecting homomorphism δ_0 in the first row of the diagram above. By the commutativity, $\chi' = \text{Cor}(\chi)$ is the image under the connecting homomorphism δ_0 of $c' = \text{Cor}(c) \in C^G$ in the second row of the diagram. By our explicit formula for the coboundary map δ_0, if $F \in M_1^G(\mathbb{Q}/\mathbb{Z})$ is any element mapping to c' in (22) then $g \cdot F - F = f_{a'}$ for a unique $a' \in \mathbb{Q}/\mathbb{Z}$, and we have $\chi'(g) = \delta_0(c')(g) = a'$ for $g \in G$. Since $f_{a'}(x) = x \cdot a' = a'$ for any $x \in G$ because G acts trivially on $\mathbb{Q}/\mathbb{Z}$, the function $g \cdot F - F$ in fact has the constant value a', and so can be evaluated at any $x \in G$ to determine the value of $\chi'(g)$.

Since $c' = \sum_{i=1}^{m} g_i \cdot c \in C^G$ where $g_1, \dots, g_m$ are representatives of the left cosets of H in G (cf. Example 4 preceding Proposition 26), such an element F is given by

$$F = \sum_{i=1}^{m} g_i \cdot f,$$

where $f \in M_1^G(\mathbb{Q}/\mathbb{Z})$ is any element mapping to c in (22). This f can be used to compute the explicit coboundary of c as before: $h \cdot f - f = f_a$ for a unique $a \in \mathbb{Q}/\mathbb{Z}$ and $\chi(h) = a$ for $h \in H$. As before, the function $h \cdot f - f = f_a$ has the constant value a and so can be evaluated at any element x of G to determine the value of $\chi(h)$.

Computing $g \cdot F - F$ on the element $1 \in G$ it follows that

$$\chi'(g) = \sum_{i=1}^{m} f(gg_i) - \sum_{i=1}^{m} f(g_i).$$

For $i = 1, \dots, m$, write

$$gg_i = g_j h(g, g_i) \qquad \text{with } h(g, g_i) \in H, \tag{17.23}$$

noting that the resulting set of g_j is some permutation of $\{g_1, \dots, g_m\}$. Then

$$\sum_{i=1}^{m} f(gg_i) - \sum_{i=1}^{m} f(g_i) = \sum_{i=1}^{m} [f(g_j h(g, g_i)) - f(g_j)] = \sum_{i=1}^{m} \chi(h(g, g_i))$$

since as noted above, $\chi(h) = f(xh) - f(x)$ for any $x \in G$. Hence

$$\chi'(g) = \chi(\prod_{i=1}^{m} h(g, g_i))$$

and so the transfer homomorphism is given by the formula

$$\text{Ver}(g) = \prod_{i=1}^{m} h(g, g_i) \tag{17.24}$$

with the elements $h(g, g_i) \in H$ defined by equation (23). Note that this proves in particular that the map defined in (24) is a homomorphism from G^{ab} to H^{ab} that is independent of the choice of representatives g_i for H in G in (23). Proving that this map is a homomorphism directly is not completely trivial. The same formula also defines the transfer homomorphism when G is infinite and H is a subgroup of finite index in G.

As an example of the transfer, suppose $H = n\mathbb{Z}$ and $G = \mathbb{Z}$ and choose $0, 1, 2, \dots, n-1$ as coset representatives for H in G. If $g = 1$, then all the elements $h(g, g_i)$ are 0 for $i = 1, 2, \dots, n-1$ and $h(1, n-1) = n$. Hence the transfer map from $\mathbb{Z}$ to $n\mathbb{Z}$ maps 1 to n, so is simply multiplication by the index. Similarly, the transfer map from any cyclic group G to a subgroup H of index n is the n^{th} power map. See also Exercise 8.

For the cyclic group $\mathbb{F}_p^\times$ for an odd prime p and subgroup $\{\pm 1\}$, it follows that the transfer map is the homomorphism $\text{Ver} : \mathbb{F}_p^\times \to \{\pm 1\}$ given by

$$\text{Ver}(a) = a^{(p-1)/2} = \left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a square} \\ -1 & \text{if } a \text{ is not a square} \end{cases}$$

(the symbol $(\frac{a}{p})$ is called the *Legendre symbol* or the *quadratic residue symbol*). If instead we take the elements $1, 2, \dots, (p-1)/2$ as coset representatives for $\{\pm 1\}$ in $\mathbb{F}_p^\times$ we see that

$$\left(\frac{a}{p}\right) = (-1)^{m(a)}$$