by each of the four elements of order 2 not in A: $\langle s \rangle$, $\langle r^2 s \rangle$, $\langle rs \rangle$ and $\langle r^3 s \rangle$. The former pair and the latter pair are conjugate in D_8 (in both cases via r), but $\langle s \rangle$ is not conjugate to $\langle rs \rangle$. Thus A has 2 conjugacy classes of complements in $A \rtimes G$ and hence $H^1(Z_2, \mathbb{Z}/4\mathbb{Z})$ has order 2. This also follows from the computation of the cohomology of cyclic groups in Section 2.

EXERCISES

1. Let G be the cyclic group of order 2 and let A be a G-module. Compute the isomorphism types of $Z^1(G, A)$, $B^1(G, A)$ and $H^1(G, A)$ for each of the following:
 (a) $A = \mathbb{Z}/4\mathbb{Z}$ (trivial action),
 (b) $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (trivial action),
 (c) $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (any nontrivial action).

2. Let p be a prime and let P be a p-group.
 (a) Show that $H^1(P, \mathbb{F}_p) \cong P/\Phi(P)$, where $\Phi(P)$ is the Frattini subgroup of P (cf. the exercises in Section 6.1).
 (b) Deduce that the dimension of $H^1(P, \mathbb{F}_p)$ as a vector space over $\mathbb{F}_p$ equals the minimum number of generators of P. [Use Exercise 26(c), Section 6.1.]

3. If G is the cyclic group of order 2 acting by inversion on $\mathbb{Z}$ show that $|H^1(G, \mathbb{Z})| = 2$. [Show that in $E = \mathbb{Z} \rtimes G$ every element of $E - \mathbb{Z}$ has order 2, and there are two conjugacy classes in this coset.]

4. Let A be the Klein 4-group and let $G = \text{Aut}(A) \cong S_3$ act on A in the natural fashion. Prove that $H^1(G, A) = 0$. [Show that in the semidirect product $E = A \rtimes G$, G is the normalizer of a Sylow 3-subgroup of E. Apply Sylow's Theorem to show all complements to A in E are conjugate.]

5. Let G be the cyclic group of order 2 acting on an elementary abelian 2-group A of order 2^n. Show that $H^1(G, A) = 0$ if and only if $n = 2k$ and $|A^G| = 2^k$. [In $E = A \rtimes G$ show that (a, x) is an element of order 2 if and only if $a \in A^G$, where $G = \langle x \rangle$. Then compare the number of complements to A with the number of E-conjugates of x.]

6. *(Thompson Transfer Lemma)* Let G be a finite group of even order, let T be a Sylow 2-subgroup of G, let $M \leq T$ with $|T : M| = 2$, and let x be an element of order 2 in G. Show that if G has no subgroup of index 2 then M contains some G-conjugate of x as follows:
 (a) Let $\text{Ver} : G/[G, G] \to T/[T, T]$ be the transfer homomorphism. Show that

$$\text{Ver}(x) = \prod_g g^{-1} x g \bmod [T, T]$$

where the product is over representatives of the cosets gT that are fixed under left multiplication by x.
 (b) Show that under left multiplication x fixes an odd number of left cosets of T in G.
 (c) Show that if G has no subgroup of index 2 then $\text{Ver}(x) \in M/[T, T]$. Deduce that for some $g \in G$ we must have $g^{-1} x g \in M$. [Consider the product $\text{Ver}(x)$ in the group T/M of order 2.]

7. Let H be a subgroup of G and let $x \in G$. The transfer $\text{Ver} : G/[G, G] \to H/[H, H]$ may be computed as follows: let $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$ be the distinct orbits of x acting by left multiplication on the left cosets of H in G, let $\mathcal{O}_i$ have length n_i and let $g_i H$ be any representative of $\mathcal{O}_i$.

(a) Show that $\mathcal{O}_i = \{g_i H, xg_i H, x^2 g_i H, \dots, x^{n_i-1} g_i H\}$ and that $g_i^{-1} x^{n_i} g_i \in H$.

(b) Show that $\mathrm{Ver}(x) = \prod_{i=1}^{k} g_i^{-1} x^{n_i} g_i \bmod [H, H]$.

8. Assume the center, $Z(G)$, of G is of index m. Prove that $\mathrm{Ver}(x) = x^m$, for all $x \in G$, where Ver is the transfer homomorphism from $G/[G,G]$ to $Z(G)$. [Use the preceding exercise.]

9. Let p be a prime, let $n \geq 3$, and let V be an n-dimensional vector space over $\mathbb{F}_p$ with basis $v_1, v_2, \dots, v_n$. Let V be a module for the symmetric group S_n, where each $\pi \in S_n$ permutes the basis in the natural way: $\pi(v_i) = v_{\pi(i)}$.

(a) Show that $|H^1(S_n, V)| = \begin{cases} 0, & \text{if } p \neq 2 \\ 2, & \text{if } p = 2 \end{cases}$. [Use Shapiro's Lemma.]

(b) Show that $H^1(A_n, V) = 0$ for all primes p.

10. Let V be the natural permutation module for S_n over $\mathbb{F}_2$, $n \geq 3$, as described in the preceding exercise, and let $W = \{a_1 v_1 + \cdots + a_n v_n \mid a_1 + \cdots + a_n = 0\}$ (the "trace zero" submodule of V). Show that if n is even then $H^1(A_n, W) \neq 0$. [Show that in the semidirect product $V \rtimes A_n$ the element v_1 induces a nontrivial outer automorphism on $E = W \rtimes A_n$ that stabilizes the series $1 \trianglelefteq W \trianglelefteq E$.]

11. Let F be a field of characteristic not dividing n and let α be any nonzero element in F. Let K be a Galois extension of F containing the splitting field of $x^n - a$, and let $\sqrt[n]{\alpha}$ be a fixed n^{th} root of α in K.

(a) Prove that $\sigma(\sqrt[n]{\alpha})/\sqrt[n]{\alpha}$ is an n^{th} root of unity.

(b) Prove that the function $f(\sigma) = \sigma(\sqrt[n]{\alpha})/\sqrt[n]{\alpha}$ is a 1-cocycle of G with values in the group μ_n of n^{th} roots of unity in K (note μ_n is not assumed to be contained in F).

(c) Prove that the 1-cocycle obtained by a different choice of n^{th} root of α in K differs from the 1-cocycle in (b) by a 1-coboundary.

12. Let F be a field of characteristic not dividing n that contains the n^{th} roots of unity, and suppose L/F is a Galois extension with abelian Galois group of exponent dividing n. Prove that L is the composite of cyclic extensions of F whose degrees are divisors of n and use this to prove that there is a bijection between the subgroups of the multiplicative group $F^\times/F^{\times^n}$ and such extensions L.

13. The Galois group of the extension $\mathbb{C}/\mathbb{R}$ is the cyclic group $G = \langle \tau \rangle$ of order 2 generated by complex conjugation τ. Prove that $H^2(G, \mathbb{C}^\times) \cong \mathbb{R}^\times/\mathbb{R}^+ \cong \mathbb{Z}/2\mathbb{Z}$ where $\mathbb{R}^+$ denotes the positive real numbers.

14. For any group G let $\hat{G} = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ denote its dual group.

(a) If $\varphi : G_1 \to G_2$ is a group homomorphism prove that composition with φ induces a homomorphism $\hat{\varphi} : \hat{G}_2 \to \hat{G}_1$ on their dual groups.

(b) For any fixed g in G, show that evaluation at g gives a homomorphism φ_g from $\hat{G}$ to $\mathbb{Q}/\mathbb{Z}$.

(c) Prove that the map taking $g \in G$ to φ_g in (b) defines a homomorphism from G to its *double dual* $\widehat{(\hat{G})}$.

(d) Prove that if G is a finite abelian group then the homomorphism in (c) is an isomorphism of G with its double dual. (By Exercise 14 in Section 5.2 the group G is (noncanonically) isomorphic to its dual $\hat{G}$. This shows that G is *canonically* isomorphic to its double dual — the isomorphism is independent of any choice of generators for G.)

(e) If $\psi : \hat{G}_2 \to \hat{G}_1$ is a homomorphism where G_1 and G_2 are finite abelian groups, then by (a) and (d) there is an induced homomorphism $\varphi : G_1 \to G_2$. Prove that

$\varphi(g_1) = g_2$ if $\chi(g_2) = \chi'(g_1)$ for $\chi' = \psi(\chi)$.

15. Use Gauss' Lemma in the computation of the transfer map for $\mathbb{F}_p^\times$ to $\{\pm 1\}$ to prove that 2 is a square modulo the odd prime p if and only if $p \equiv \pm 1 \bmod 8$. [Count how many elements in $2, 4, \ldots, p-1$ are greater than $(p-1)/2$.]

17.4 GROUP EXTENSIONS, FACTOR SETS AND $H^2(G,A)$

If A is a G-module then from the definition of the coboundary map d_2 in equation (18) a function f from $G \times G$ to A is a 2-cocycle if it satisfies the identity

$$f(g,h) + f(gh,k) = g \cdot f(h,k) + f(g,hk) \qquad \text{for all } g,h,k \in G. \tag{17.26}$$

Equivalently, a 2-cocycle is determined by a collection of elements $\{a_{g,h}\}_{g,h \in G}$ of elements in A satisfying $a_{g,h} + a_{gh,k} = g \cdot a_{h,k} + a_{g,hk}$ for $g,h,k \in G$ (and then the 2-cocycle f is the function sending (g,h) to $a_{g,h}$).

A 2-cochain f is a coboundary if there is a function $f_1 : G \to A$ such that

$$f(g,h) = gf_1(h) - f_1(gh) + f_1(g), \qquad \text{for all } g,h \in G \tag{17.27}$$

i.e., f is the image under d_1 of the 1-cochain f_1.

One of the main results of this section is to make a connection between the 2-cocycles $Z^2(G,A)$ and the *factor sets* associated to a group extension of G by A, which arise when considering the effect of choosing different coset representatives in defining the multiplication in the extension. In particular, we shall show that there is a bijection between equivalence classes of group extensions of G by A (with the action of G on A fixed) and the elements of $H^2(G,A)$.

We first observe some basic facts about extensions. Let E be any group extension of G by A,

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1. \tag{17.28}$$

The extension (28) determines an action of G on A, as follows. For each $g \in G$ let e_g be an element of E mapping onto g by π (the choice of such a set of representatives for G in E is called a set-theoretic *section* of π). The element e_g acts by conjugation on the normal subgroup $\iota(A)$ of E, mapping $\iota(a)$ to $e_g\iota(a)e_g^{-1}$. Any other element in E that maps to g is of the form $e_g\iota(a_1)$ for some $a_1 \in A$, and since $\iota(A)$ is abelian, conjugation by this element on $\iota(A)$ is the same as conjugation by e_g, so is independent of the choice of representative for g. Hence G acts on $\iota(A)$, and so also on A since ι is injective. Since conjugation is an automorphism, the extension (28) defines A as a G-module.

Recall from Section 10.5 that two extensions $1 \to A \xrightarrow{\iota_1} E_1 \xrightarrow{\pi_1} G \to 1$ and $1 \to A \xrightarrow{\iota_2} E_2 \xrightarrow{\pi_2} G \to 1$ are *equivalent* if there is a group isomorphism $\beta : E_1 \to E_2$ such that the following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\iota_1"] \arrow[d, "\mathrm{id}"] & E_1 \arrow[r, "\pi_1"] \arrow[d, "\beta"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A \arrow[r, "\iota_2"] & E_2 \arrow[r, "\pi_2"] & G \arrow[r] & 1.
\end{tikzcd} \tag{17.29}$$