Stab$(1 \trianglelefteq \iota(A) \trianglelefteq E)$. (Thus Proposition 31 implies $Z^1(G, A)$ is the group of equivalences of the extension with itself).

6. *(Gaschütz's Theorem)* Let p be a prime, let A be an abelian normal p-subgroup of a finite group G, and let P be a Sylow p-subgroup of G. Prove that G is a split extension of G/A by A if and only if P is a split extension of P/A by A. (Note that $A \leq P$ by Exercise 37 in Section 4.5). [Use Sylow's Theorem to show if G splits over A then so too does P. Conversely, show that a normalized 2-cocycle associated to the extension of P/A by A via Theorem 36 is the image of a normalized 2-cocycle in $H^2(G/A, A)$ under the restriction homomorphism Res : $H^2(G/A, A) \to H^2(P/A, A)$. Then use Proposition 26 and the fact that multiplication by $|G : P|$ is an automorphism of A.]

7. **(a)** Prove that $H^2(A_4, \mathbb{Z}/2\mathbb{Z}) \neq 0$ by exhibiting a nonsplit extension of A_4 by a cyclic group of order 2. [See Exercise 11, Section 4.5.]
   (b) Prove that $H^2(A_5, \mathbb{Z}/2\mathbb{Z}) \neq 0$ by showing that $SL_2(\mathbb{F}_5)$ is a nonsplit extension of A_5 by a cyclic group of order 2. [Use Propositions 21 and 23 in Section 4.5.]

8. The *Schur multiplier* of a finite group G is defined as the group $H^2(G, \mathbb{C}^\times)$, where the multiplicative group $\mathbb{C}^\times$ of complex numbers is a trivial G-module. Prove that the Schur multiplier is a finite group. [Show that every cohomology class contains a cocycle whose values lie in the n^{th} roots of unity, where $n = |G|$, as follows: If f is any cocycle then by Corollary 27, $f^n \in B^2(G, \mathbb{C}^\times)$. Define $k \in C^2(G, \mathbb{C}^\times)$ by $k(g_1, g_2) = f(g_1, g_2)^{1/n}$ (take any n^{th} roots). Show that $k \in B^2(G, \mathbb{C}^\times)$ and fk^{-1} takes values in the group of n^{th} roots of 1.]

9. Use the classification of the extensions of the Klein 4-group by Z_2 in the example following Theorem 39 to prove the following (in the notation of that example):
   (a) There is an (outer) automorphism of $Z_4 \times Z_2$ which interchanges the cosets Ax and Axy and fixes the coset Ay.
   (b) There is an outer automorphism of D_8 which interchanges the cosets As and Asr and fixes the coset Ar.

10. Suppose $\mathbb{F}_q$ is a finite field with $G = \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \sigma_q \rangle$ where σ_q is the Frobenius automorphism, and let N be the usual norm element for the cyclic group G.
    (a) Use Hilbert's Theorem 90 to prove that $|_N(\mathbb{F}_{q^d}^\times)| = (q^d - 1)/(q - 1)$, and deduce that the norm map from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$ is surjective.
    (b) Prove that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all $n \geq 1$.

Part VI

INTRODUCTION TO THE REPRESENTATION THEORY OF FINITE GROUPS

The final two chapters are an introduction to the representation theory of finite groups together with some applications. We have already seen in Part I how actions of groups on sets, namely permutation representations, are a fundamental tool for unravelling the structure of groups. Cayley's Theorem and Sylow's Theorem as well as many of the results and applications in Sections 6.1 and 6.2 are based on groups acting on sets. The chapter on Galois Theory developed one of the most beautiful correspondences in mathematics where the action of a group as automorphisms of a field gives rise to a correspondence between the lattice of subgroups of the Galois group and the lattice of subfields of a Galois extension of fields. In these final two chapters we study groups acting as linear transformations on vector spaces. We shall be primarily interested in utilizing these linear actions to provide information about the groups themselves.

In Part III we saw that modules are the "representation objects" for rings in the sense that the axioms for an R-module specify a "ring action" of R on some abelian group M which preserves the abelian group structure of M. In the case where M was an $F[x]$-module, x acted as a linear transformation from the vector space M to itself. In Chapter 12 the classification of finitely generated modules over Principal Ideal Domains gave us a great deal of information about these linear transformations of M (e.g., canonical forms). In Chapter 16 we used the ideal structure in Dedekind Domains to generalize the results of Chapter 12 to the classification of finitely generated modules over such domains. In this part we follow a process similar to the study of $F[x]$-modules, replacing the polynomial ring with the group ring FG of G and classifying all finitely generated FG-modules for certain fields F (Wedderburn's Theorem). We then use this classification to derive some results about finite groups such as Burnside's Theorem on the solvability of groups of order $p^a q^b$ in Chapter 19.

CHAPTER 18

Representation Theory and Character Theory

18.1 LINEAR ACTIONS AND MODULES OVER GROUP RINGS

For the remainder of the book the groups we consider will be finite groups, unless explicitly mentioned otherwise. Throughout this section F is a field and G is a finite group. We first introduce the basic terminology. Recall that if V is a vector space over F, then $GL(V)$ is the group of nonsingular linear transformations from V to itself (under composition), and if $n \in \mathbb{Z}^+$, then $GL_n(F)$ is the group of invertible $n \times n$ matrices with entries from F (under matrix multiplication).

Definition. Let G be a finite group, let F be a field and let V be a vector space over F.

(1) A *linear representation* of G is any homomorphism from G into $GL(V)$. The *degree* of the representation is the dimension of V.

(2) Let $n \in \mathbb{Z}^+$. A *matrix representation* of G is any homomorphism from G into $GL_n(F)$.

(3) A linear or matrix representation is *faithful* if it is injective.

(4) The *group ring* of G over F is the set of all formal sums of the form

$$\sum_{g \in G} \alpha_g g, \qquad \alpha_g \in F$$

with componentwise addition and multiplication $(\alpha g)(\beta h) = (\alpha\beta)(gh)$ (where α and β are multiplied in F and gh is the product in G) extended to sums via the distributive law (cf. Section 7.2).

Unless we are specifically discussing permutation representations the term "representation" will always mean "linear representation." When we wish to emphasize the field F we shall say F-representation, or representation of G on V over F.

Recall that if V is a finite dimensional vector space of dimension n, then by fixing a basis of V we obtain an isomorphism $GL(V) \cong GL_n(F)$. In this way any linear representation of G on a finite dimensional vector space gives a matrix representation and vice versa. For the most part our linear representations will be of finite degree and we shall pass freely between linear representations and matrix representations (specifying a

basis when we wish to give an explicit correspondence between the two). Furthermore, given a linear representation $\varphi : G \to GL(V)$ of finite degree, a corresponding matrix representation provides numerical invariants (such as the determinant of $\varphi(g)$ for $g \in G$) which are independent of the choice of basis giving the isomorphism between $GL(V)$ and $GL_n(F)$. The exploitation of such invariants will be fundamental to our development.

Before giving examples of representations we recall the group ring FG in greater detail (group rings were introduced in Section 7.2, and some notation and examples were discussed in that section). Suppose the elements of G are $g_1, g_2, \ldots, g_n$. Each element of FG is of the form

$$\sum_{i=1}^{n} \alpha_i g_i, \qquad \alpha_i \in F.$$

Two formal sums[1] are equal if and only if all corresponding coefficients of group elements are equal. Addition and multiplication in FG are defined as follows:

$$\sum_{i=1}^{n} \alpha_i g_i \quad + \quad \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i$$

$$\left(\sum_{i=1}^{n} \alpha_i g_i\right)\left(\sum_{i=1}^{n} \beta_i g_i\right) = \sum_{k=1}^{n} \left(\sum_{\substack{i,j \\ g_i g_j = g_k}} \alpha_i \beta_j \right) g_k$$

where addition and multiplication of the coefficients α_i and β_j is performed in F. Note that by definition of multiplication,

FG is a commutative ring if and only if G is an abelian group.

The group G appears in FG (identifying g_i with $1g_i$) and the field F appears in FG (identifying β with βg_1, where g_1 is the identity of G). Under these identifications

$$\beta\left(\sum_{i=1}^{n} \alpha_i g_i\right) = \sum_{i=1}^{n} (\beta\alpha_i) g_i, \qquad \text{for all } \beta \in F.$$

In this way

FG is a vector space over F with the elements of G as a basis.

In particular, FG is a vector space over F of dimension equal to $|G|$. The elements of F commute with all elements of FG, i.e., F is in the *center* of FG. When we wish to emphasize the latter two properties we shall say that FG is an *F-algebra* (in general, an F-algebra is a ring R which contains F in its center, so R is both a ring and an F-vector space).

Note that the operations in FG are similar to those in the F-algebra $F[x]$ (although $F[x]$ is infinite dimensional over F). In some works FG is denoted by $F[G]$, although the latter notation is currently less prevalent.

---

[1]The formal sum displayed above is a way of writing the function from G to F which takes the value α_i on the group element g_i. This same "formality" was used in the construction of free modules (see Theorem 6 in Section 10.3).