

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

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

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

Corollary 14
Ch 11
Page 48
468

basis when we wish to give an explicit correspondence between the two). Furthermore, given a linear representation $\varphi : G \rightarrow GL(V)$ 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, \dots, g_n . Each element of FG is of the form

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

Two formal sums¹ are equal if and only if all corresponding coefficients of group elements are equal. Addition and multiplication in FG are defined as follows:

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

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

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

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.

¹The 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).

Examples

- (1) If $G = \langle g \rangle$ is cyclic of order $n \in \mathbb{Z}^+$, then the elements of FG are of the form

$$\sum_{i=0}^{n-1} \alpha_i g^i.$$

The map $F[x] \rightarrow F\langle g \rangle$ which sends x^k to g^k for all $k \geq 0$ extends by F -linearity to a surjective ring homomorphism with kernel equal to the ideal generated by $x^n - 1$. Thus

$$F\langle g \rangle \cong F[x]/(x^n - 1).$$

This is an isomorphism of F -algebras, i.e., is a ring isomorphism which is F -linear.

- (2) Under the notation of the preceding example let $r = 1 + g + g^2 + \cdots + g^{n-1}$, so r is a nonzero element of $F\langle g \rangle$. Note that $rg = g + g^2 + \cdots + g^{n-1} + 1 = r$, hence $r(1 - g) = 0$. Thus the ring $F\langle g \rangle$ contains zero divisors (provided $n > 1$). More generally, if G is any group of order > 1 , then for any nonidentity element $g \in G$, $F\langle g \rangle$ is a subring of FG , so FG also contains zero divisors.
- (3) Let $G = S_3$ and $F = \mathbb{Q}$. The elements $r = 5(1\ 2) - 7(1\ 2\ 3)$ and $s = -4(1\ 2\ 3) + 12(1\ 3\ 2)$ are typical members of $\mathbb{Q}S_3$. Their sum and product are seen to be

$$\begin{aligned} r + s &= 5(1\ 2) - 11(1\ 2\ 3) + 12(1\ 3\ 2) \\ rs &= -20(2\ 3) + 28(1\ 3\ 2) + 60(1\ 3) - 84 \end{aligned}$$

(recall that products (compositions) of permutations are computed from right to left). An explicit example of a sum and product of two elements in the group ring $\mathbb{Q}D_8$ appears in Section 7.2.

Before giving specific examples of representations we discuss the correspondence between representations of G and FG -modules (after which we can simultaneously give examples of both). This discussion closely parallels the treatment of $F[x]$ -modules in Section 10.1.

Suppose first that $\varphi : G \rightarrow GL(V)$ is a representation of G on the vector space V over F . As above, write $G = \{g_1, \dots, g_n\}$, so for each $i \in \{1, \dots, n\}$, $\varphi(g_i)$ is a linear transformation from V to itself. Make V into an FG -module by defining the action of a ring element on an element of V as follows:

$$\left(\sum_{i=1}^n \alpha_i g_i \right) \cdot v = \sum_{i=1}^n \alpha_i \varphi(g_i)(v), \quad \text{for all } \sum_{i=1}^n \alpha_i g_i \in FG, \ v \in V.$$

We verify a special case of axiom 2(b) of a module (see Section 10.1) which shows precisely where the fact that φ is a group homomorphism is needed:

$$\begin{aligned} (g_i g_j) \cdot v &= \varphi(g_i g_j)(v) && \text{(by definition of the action)} \\ &= (\varphi(g_i) \circ \varphi(g_j))(v) && \text{(since } \varphi \text{ is a group homomorphism)} \\ &= \varphi(g_i)(\varphi(g_j)(v)) && \text{(by definition of a composition of linear transformations)} \\ &= g_i \cdot (g_j \cdot v) && \text{(by definition of the action).} \end{aligned}$$

missions associated with a product or an
ties are equal to zero. A product can only be
for all

This argument extends by linearity to arbitrary elements of FG to prove that axiom 2(b) of a module holds in general. It is an exercise to check that the remaining module axioms hold.

Note that F is a subring of FG and the action of the field element α on a vector is the same as the action of the ring element $\alpha 1$ on a vector i.e., the FG -module action extends the F action on V .

Suppose now that conversely we are given an FG -module V . We obtain an associated vector space over F and representation of G as follows. Since V is an FG -module, it is an F -module, i.e., it is a vector space over F . Also, for each $g \in G$ we obtain a map from V to V , denoted by $\varphi(g)$, defined by

$$\varphi(g)(v) = g \cdot v \quad \text{for all } v \in V,$$

where $g \cdot v$ is the given action of the ring element g on the element v of V . Since the elements of F commute with each $g \in G$ it follows by the axioms for a module that for all $v, w \in V$ and all $\alpha, \beta \in F$ we have

$$\begin{aligned} \varphi(g)(\alpha v + \beta w) &= g \cdot (\alpha v + \beta w) \\ &= g \cdot (\alpha v) + g \cdot (\beta w) \\ &= \alpha(g \cdot v) + \beta(g \cdot w) \\ &= \alpha\varphi(g)(v) + \beta\varphi(g)(w), \end{aligned}$$

that is, for each $g \in G$, $\varphi(g)$ is a linear transformation. Furthermore, it follows by axiom 2(b) of a module that

$$\varphi(g_i g_j)(v) = (\varphi(g_i) \circ \varphi(g_j))(v)$$

(this is essentially the calculation above with the steps reversed). This proves that φ is a group homomorphism (in particular, $\varphi(g^{-1}) = \varphi(g)^{-1}$, so every element of G maps to a nonsingular linear transformation, i.e., $\varphi : G \rightarrow GL(V)$).

This discussion shows there is a bijection between FG -modules and pairs (V, φ) :

$$\left\{ \begin{array}{l} V \text{ an } FG\text{-module} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} V \text{ a vector space over } F \\ \text{and} \\ \varphi : G \rightarrow GL(V) \text{ a representation} \end{array} \right\}.$$

Giving a representation $\varphi : G \rightarrow GL(V)$ on a vector space V over F is therefore equivalent to giving an FG -module V . Under this correspondence we shall say that the module V *affords* the representation φ of G .

Recall from Section 10.1 that if a vector space M is made into an $F[x]$ -module via the linear transformation T , then the $F[x]$ -submodules of M are precisely the T -stable subspaces of M . In the current situation if V is an FG -module affording the representation φ , then a subspace U of V is called *G-invariant* or *G-stable* if $g \cdot u \in U$ for all $g \in G$ and all $u \in U$ (i.e., if $\varphi(g)(u) \in U$ for all $g \in G$ and all $u \in U$). It follows easily that

the FG -submodules of V are precisely the G -stable subspaces of V .