

1.3.1. *homomorphisms.* In order to prove Maschke's theorem, we need to talk about homomorphisms of G -modules. We can define these to be the same as homomorphisms of $k[G]$ -modules. Then the following is a proposition. (Or, we can take the following as the definition of a G -module homomorphism, in which case the proposition is that G -module homomorphisms are the same as homomorphisms of $k[G]$ -modules.)

Proposition 1.11. *Suppose that V, W are $k[G]$ -modules. Then a k -linear mapping $\phi : V \rightarrow W$ is a homomorphism of $k[G]$ -modules if and only if it commutes with the action of G . I.e., if*

$$\sigma(\phi(v)) = \phi(\sigma v)$$

for all $\sigma \in G$.

Proof. Any homomorphism of $k[G]$ -modules will commute with the action of $k[G]$ and therefore with the action of $G \subset k[G]$. Conversely, if $\phi : V \rightarrow W$ commutes with the action of G then, for any $\sum a_\sigma \sigma \in k[G]$, we have

$$\phi \left(\sum_{\sigma \in G} a_\sigma \sigma v \right) = \sum_{\sigma \in G} a_\sigma \phi(\sigma v) = \sum_{\sigma \in G} a_\sigma \sigma \phi(v) = \left(\sum_{\sigma \in G} a_\sigma \sigma \right) \phi(v)$$

So, ϕ is a homomorphism of $k[G]$ -modules. \square

We also have the following Proposition/Definition of a G -submodule.

Proposition 1.12. *A subset W of a G -module V over k is a $k[G]$ -submodule (and we call it a G -submodule) if and only if*

- (1) W is a vector subspace of V and
- (2) W is invariant under the action of G . I.e., $\sigma W \subseteq W$ for all $\sigma \in G$.

Proof of Maschke's Theorem. Suppose that V is a finitely generated G -module and W is any G -submodule of V . Then we want to show that W is a direct summand of V . This is one of the characterizations of semisimple modules. This will prove that all f.g. $k[G]$ -modules are semisimple and therefore $k[G]$ is a semisimple ring.

Since W is a submodule of V , it is in particular a vector subspace of V . So, there is a linear projection map $\phi : V \rightarrow W$ so that $\phi|_W = id_W$. If ϕ is a homomorphism of G -modules, then $V = W \oplus \ker \phi$ and W would split from V . So, we would be done. If ϕ is not a G -homomorphism, we can make it into a G -homomorphism by "averaging over the group," i.e., by replacing it with $\psi = \frac{1}{n} \sum \lambda_{\sigma^{-1}} \circ \phi \circ \lambda_\sigma$.

First, I claim that $\psi|_W = id_W$. To see this take any $w \in W$. Then $\sigma w \in W$. So, $\phi(\sigma w) = \sigma w$ and

$$\psi(w) = \frac{1}{n} \sum_{\sigma \in G} \sigma^{-1} \phi(\sigma w) = \frac{1}{n} \sum_{\sigma \in G} \sigma^{-1}(\sigma w) = w$$

Next I claim that ψ is a homomorphism of G -modules. To show this take any $\tau \in G$ and $v \in V$. Then

$$\begin{aligned} \psi(\tau v) &= \frac{1}{n} \sum_{\sigma \in G} \sigma^{-1} \phi(\sigma \tau v) = \frac{1}{n} \sum_{\alpha \beta = \tau} \alpha \phi(\beta v) \\ &= \frac{1}{n} \sum_{\sigma \in G} \tau \sigma^{-1} \phi(\sigma v) = \tau \psi(v) \end{aligned}$$

So, ψ gives a splitting of V as required. □

1.3.2. $\mathbb{R}[\mathbb{Z}/3]$. I gave a longwinded explanation of Example 1.10 using the universal property of the group ring $k[G]$. In these notes, I will just summarize this property in one equation. If R is any k -algebra and $U(R)$ is the group of units of R , then:

$$\text{Hom}_{k\text{-alg}}(k[G], R) \cong \text{Hom}_{grp}(G, U(R))$$

The isomorphism is given by restriction and linear extension.

The isomorphism $\mathbb{R}[\mathbb{Z}/3] \cong \mathbb{R} \times \mathbb{C}$ is given by the mapping:

$$\phi : \mathbb{Z}/3 \rightarrow \mathbb{R} \times \mathbb{C}$$

which sends the generator σ to $(1, \omega)$ where ω is a primitive third root of unity. Since $(1, 0), (1, \omega), (1, \bar{\omega})$ are linearly independent over \mathbb{R} , the linear extension $\bar{\phi}$ of ϕ is an isomorphism of \mathbb{R} -algebras.

1.3.3. *group rings over \mathbb{C}* . We will specialize to the case $k = \mathbb{C}$. In that case, there are no finite dimensional division algebras over \mathbb{C} (Part C, Theorem 3.12). So, we get only matrix algebras:

Corollary 1.13. *If G is any finite group then*

$$\mathbb{C}[G] \cong \text{Mat}_{d_1}(\mathbb{C}) \times \cdots \times \text{Mat}_{d_b}(\mathbb{C})$$

In particular, $n = |G| = \sum d_i^2$.

Example 1.14. *If G is a finite abelian group of order n then $\mathbb{C}[G] \cong \mathbb{C}^n$.*

Example 1.15. Take $G = S_3$, the symmetric group on 3 letters. Since this group is nonabelian, the numbers d_i cannot all be equal to 1. But the only way that 6 can be written as a sum of squares, not all 1, is $6 = 1 + 1 + 4$. Therefore,

$$\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times \text{Mat}_2(\mathbb{C})$$

This can be viewed as a subalgebra of $\text{Mat}_4(\mathbb{C})$ given by

$$\begin{pmatrix} * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix}$$

Each star (*) represents an independent complex variable. In this description, it is easy to visualize what are the simple factors $\text{Mat}_{d_i}(\mathbb{C})$ given by the Wedderburn structure theorem. But what are the corresponding factors of the group ring $\mathbb{C}[G]$?

1.4. idempotents. Suppose that $R = R_1 \times R_2 \times R_3$ is a product of three subrings. Then the unity of R decomposes as $1 = (1, 1, 1)$. This can be written as a sum of unit vectors:

$$1 = (1, 0, 0) + (0, 1, 0) + (0, 0, 1) = e_1 + e_2 + e_3$$

This is a decomposition of unity (1) as a sum of central, orthogonal idempotents e_i .

Recall that *idempotent* means that $e_i^2 = e_i$ for all i . Also, 0 is not considered to be an idempotent. *Orthogonal* means that $e_i e_j = 0$ if $i \neq j$. *Central* means that $e_i \in Z(R)$.

Theorem 1.16. A ring R can be written as a product of b subrings R_1, R_2, \dots, R_b iff $1 \in R$ can be written as a sum of b central, orthogonal idempotents and, in that case, $R_i = e_i R$.

A central idempotent e is called *primitive* if it cannot be written as a sum of two central orthogonal idempotents.

Corollary 1.17. The number of factors $R_i = e_i R$ is maximal iff each e_i is primitive.

So, the problem is to write unity $1 \in \mathbb{C}[G]$ as a sum of primitive, central (\Rightarrow orthogonal) idempotents. We will derive a formula for this decomposition using characters.