

1. THE GROUP RING $k[G]$

The main idea is that representations of a group G over a field k are “the same” as modules over the group ring $k[G]$. First I defined both terms.

1.1. Representations of groups.

Definition 1.1. A representation of a group G over a field k is defined to be a group homomorphism

$$\rho : G \rightarrow \text{Aut}_k(V)$$

where V is a vector space over k .

Here $\text{Aut}_k(V)$ is the group of k -linear automorphisms of V . This is also written as $GL_k(V)$. This is the group of units of the ring $\text{End}_k(V) = \text{Hom}_k(V, V)$ which, as I explained before, is a ring with addition defined pointwise and multiplication given by composition. If $\dim_k(V) = d$ then $\text{Aut}_k(V) \cong \text{Aut}_k(k^d) = GL_d(k)$ which can also be described as the group of units of the ring $\text{Mat}_d(k)$ or as:

$$GL_d(k) = \{A \in \text{Mat}_d(k) \mid \det(A) \neq 0\}$$

$d = \dim_k(V)$ is called the *dimension* of the representation ρ .

1.1.1. examples.

Example 1.2. The first example I gave was the *trivial representation*. This is usually defined to be the one dimensional representation $V = k$ with trivial action of the group G (which can be arbitrary). *Trivial action* means that $\rho(\sigma) = 1 = id_V$ for all $\sigma \in G$.

In the next example, I pointed out that the group G needs to be written multiplicatively no matter what.

Example 1.3. Let $G = \mathbb{Z}/3$. Written multiplicatively, the elements are $1, \sigma, \sigma^2$. Let $k = \mathbb{R}$ and let $V = \mathbb{R}^2$ with $\rho(\sigma)$ defined to be rotation by $120^\circ = 2\pi/3$. I.e.,

$$\rho(\sigma) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$$

Example 1.4. Suppose that E is a field extension of k and $G = \text{Gal}(E/k)$. Then G acts on E by k -linear transformations. This gives a representation:

$$\rho : G \hookrightarrow \text{Aut}_k(E)$$

Note that this map is an inclusion by definition of “Galois group.”

1.1.2. *axioms.* In an elementary discussion of group representations I would write a list of axioms as a definition. However, they are just longwinded explanations of what it means for $\rho : G \rightarrow \text{Aut}_k(V)$ to be a group homomorphism. The only advantage is that you don't need to assume that $\rho(\sigma)$ is an automorphism. Here are the axioms. (I switched the order of (2) and (3) in the lecture.)

- (1) $\rho(1) = 1$ $1v = v \quad \forall v \in V$
- (2) $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau) \quad \forall \sigma, \tau \in G$ $(\sigma\tau)v = \sigma(\tau v) \quad \forall v \in V$
- (3) $\rho(\sigma)$ is k -linear $\forall \sigma \in G$ $\sigma(av + bw) = a\sigma v + b\sigma w \quad \forall v, w \in V, a, b \in k$

The first two conditions say that ρ is an *action* of G on V . Actions are usually written by juxtaposition:

$$\sigma v := \rho(\sigma)(v)$$

The third condition says that the action is k -linear. So, together, the axioms say that a representation of G is a k -linear action of G on a vector space V .

1.2. **Modules over $k[G]$.** The *group ring* $k[G]$ is defined to be the set of all finite k linear combinations of elements of G : $\sum a_\sigma \sigma$ where $a_\sigma \in k$ for all $\sigma \in G$ and $a_\sigma = 0$ for almost all σ .

For example, $\mathbb{R}[\mathbb{Z}/3]$ is the set of all linear combinations

$$x + y\sigma + z\sigma^2$$

where $x, y, z \in \mathbb{R}$. I.e., $\mathbb{R}[\mathbb{Z}/3] \cong \mathbb{R}^3$. In general $k[G]$ is a vector space over k with G as a basis.

Multiplication in $k[G]$ is given by

$$\left(\sum a_\sigma \sigma\right) \left(\sum b_\tau \tau\right) = \left(\sum c_\lambda \lambda\right)$$

where $c_\lambda \in k$ can be given in three different ways:

$$c_\lambda = \sum_{\sigma\tau=\lambda} a_\sigma b_\tau = \sum_{\sigma \in G} a_\sigma b_{\sigma^{-1}\lambda} = \sum_{\tau \in G} a_{\lambda\tau^{-1}} b_\tau$$

Proposition 1.5. $k[G]$ is a k -algebra.

This is straightforward and tedious. So, I didn't prove it. But I did explain what it means and why it is important.

Recall that an *algebra* over k is a ring which contains k in its center. The *center* $Z(R)$ of a (noncommutative) ring R is defined to be the set of elements of R which commute with all the other elements:

$$Z(R) := \{x \in R \mid xy = yx \quad \forall y \in R\}$$

$Z(R)$ is a subring of R .

The center is important for the following reason. Suppose that M is a (left) R -module. Then each element $r \in R$ acts on M by left multiplication λ_r

$$\lambda_r : M \rightarrow M, \quad \lambda_r(x) = rx$$

This is a homomorphism of $Z(R)$ -modules since:

$$\lambda_r(ax) = rax = arx = a\lambda_r(x) \quad \forall a \in Z(R)$$

Thus the action of R on M gives a ring homomorphism:

$$\rho : R \rightarrow \text{End}_{Z(R)}(M)$$

Getting back to $k[G]$, suppose that M is a $k[G]$ -module. Then the action of $k[G]$ on M is k -linear since k is in the center of $k[G]$. So, we get a ring homomorphism

$$\rho : k[G] \rightarrow \text{End}_k(M)$$

This restricts to a group homomorphism

$$\rho|_G : G \rightarrow \text{Aut}_k(M)$$

I pointed out that, in general, any ring homomorphism $\phi : R \rightarrow S$ will induce a group homomorphism $U(R) \rightarrow U(S)$ where $U(R)$ is the group of units of R . And I pointed out earlier that $\text{Aut}_k(M)$ is the group of units of $\text{End}_k(M)$. G is contained in the group of units of $k[G]$. (An interesting related question is: Which finite groups occur as groups of units of rings?)

This discussion shows that a $k[G]$ -module M gives, by restriction, a representation of the group G on the k -vector space M . Conversely, suppose that

$$\rho : G \rightarrow \text{Aut}_k(V)$$

is a group representation. Then we can extend ρ to a ring homomorphism

$$\bar{\rho} : k[G] \rightarrow \text{End}_k(V)$$

by the simple formula

$$\bar{\rho} \left(\sum a_\sigma \sigma \right) = \sum a_\sigma \rho(\sigma)$$

When we say that a representation of a group G is “the same” as a $k[G]$ -module we are talking about this correspondence. The vector space V is also called a G -module. So, it would be more accurate to say that a G -module is the same as a $k[G]$ -module.

Corollary 1.6. (1) *Any group representation $\rho : G \rightarrow \text{Aut}_k(V)$ extends uniquely to a ring homomorphism $\bar{\rho} : k[G] \rightarrow \text{End}_k(V)$ making V into a $k[G]$ -module.*

- (2) For any $k[G]$ -module M , the action of $k[G]$ on M restricts to give a group representation $G \rightarrow \text{Aut}_k(M)$.
- (3) These two operations are inverse to each other in the sense that ρ is the restriction of $\bar{\rho}$ and an action of the ring $k[G]$ is the unique extension of its restriction to G .

There are some conceptual differences between the group representation and the corresponding $k[G]$ -module. For example, the module might not be faithful even if the group representation is:

Definition 1.7. A group representation $\rho : G \rightarrow \text{Aut}_k(V)$ is called *faithful* if only the trivial element of G acts as the identity on V . I.e., if the kernel of ρ is trivial. An R -module M is called *faithful* if the annihilator of M is zero. ($\text{ann}(M) = \{r \in R \mid rx = 0 \forall x \in M\}$).

These two definitions do not agree. For example, take the representation

$$\rho : \mathbb{Z}/3 \hookrightarrow GL_2(\mathbb{R})$$

which we discussed earlier. This is faithful. But the extension to a ring homomorphism

$$\bar{\rho} : \mathbb{R}[\mathbb{Z}/3] \rightarrow \text{Mat}_2(\mathbb{R})$$

is not a monomorphism since $1 + \sigma + \sigma^2$ is in its kernel.

1.3. Semisimplicity of $k[G]$. The main theorem about $k[G]$ is the following.

Theorem 1.8 (Maschke). *If G is a finite group of order $|G| = n$ and k is a field with $\text{char } k \nmid n$ (or $\text{char } k = 0$) then $k[G]$ is semisimple.*

Instead of saying $\text{char } k$ is either 0 or a prime not dividing n , I will say that $1/n \in k$. By the Wedderburn structure theorem we get the following.

Corollary 1.9. *If $1/|G| \in k$ then*

$$k[G] \cong \text{Mat}_{d_1}(D_1) \times \cdots \times \text{Mat}_{d_b}(D_b)$$

where D_i are finite dimensional division algebras over k .

Example 1.10.

$$\mathbb{R}[\mathbb{Z}/3] \cong \mathbb{R} \times \mathbb{C}$$

In general, if G is abelian, then the numbers d_i must all be 1 and D_i must be finite field extensions of k .

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.

1.5. **Center of $\mathbb{C}[G]$.** Before I move on to characters, I want to prove one last thing about the group ring $\mathbb{C}[G]$.

Theorem 1.18. *The number of factors b in the decomposition*

$$\mathbb{C}[G] \cong \prod_{i=1}^b \text{Mat}_{d_i}(\mathbb{C})$$

is equal to the number of conjugacy classes of elements of G .

For, example, the group S_3 has three conjugacy classes: the identity $\{1\}$, the transpositions $\{(12), (23), (13)\}$ and the 3-cycles $\{(123), (132)\}$.

In order to prove this we note that b is the dimension of the center of the right hand side. Any central element of $\text{Mat}_{d_i}(\mathbb{C})$ is a scalar multiple of the unit matrix which we are calling e_i (the i th primitive central idempotent). Therefore:

Lemma 1.19. *The center of $\prod_{i=1}^b \text{Mat}_{d_i}(\mathbb{C})$ is the vector subspace spanned by the primitive central idempotents e_1, \dots, e_b . In particular it is b -dimensional.*

So, it suffices to show that the dimension of the center of $\mathbb{C}[G]$ is equal to the number of conjugacy classes of elements of G . (If G is abelian, this is clearly true.)

Definition 1.20. A *class function* on G is a function $f : G \rightarrow X$ so that f takes the same value on conjugate elements. I.e.,

$$f(\tau\sigma\tau^{-1}) = f(\sigma)$$

for all $\sigma, \tau \in G$. Usually, $X = \mathbb{C}$.

For example, any function on an abelian group is a class function.

Lemma 1.21. *For any field k , the center of $k[G]$ is the set of all $\sum_{\sigma \in G} a_\sigma \sigma$ so that a_σ is a class function on G . So, $Z(k[G]) \cong k^c$ where c is the number of conjugacy classes of elements of G .*

Proof. If $\sum_{\sigma \in G} a_\sigma \sigma$ is central then

$$\sum_{\sigma \in G} a_\sigma \sigma = \tau \sum_{\sigma \in G} a_\sigma \sigma \tau^{-1} = \sum_{\sigma \in G} a_\sigma \tau \sigma \tau^{-1}$$

The coefficient of $\tau\sigma\tau^{-1}$ on both sides must agree. So

$$a_{\tau\sigma\tau^{-1}} = a_\sigma$$

I.e., a_σ is a class function. The converse is also clear. □

These two lemmas clearly imply Theorem 1.18 (which can now be stated as: $b = c$ if $k = \mathbb{C}$).