Faculty of Natural Sciences
University of Copenhagen

Modern Algebra 2006

The correspondence between representations of a finite group and modules over its group ring

Eva Rotenberg, Anders Storm Hansen

Lecture notes for: 2 October 2006

Foreword

We start with a short summary of the theory involved, based on [Jøndrup06a], [Jøndrup06b] and [Foxby04]. Please confer the mentioned lecture notes for further information on the subjects.

Complex representations

Definition 1 (Representation of a finite group.)**.** Given a group, $(G, \star)$, with identity element 1_G and given a vector space, V, over a field, k, a *representation* is a map

$$T : G \to \mathrm{Hom}_k(V, V) \text{ such that}$$

$$T(1_G) = 0_V \text{ and}$$

$$T(g \star h) = T(g)T(h)$$

In case k equals the complex numbers, $\mathbb{C}$, we say T is a *complex representation*.

The *dimension* of a representation $T : G \to \mathrm{Hom}_k(V, V)$ is the dimension of the vector space V.

Definition 2 (Morphism of representations)**.** Let $T : G \to \mathrm{End}_{\mathbb{C}}(V)$ and $S : G \to \mathrm{End}_{\mathbb{C}}(W)$ be representations of the finite group G.

A *morphism of representations* from T to S is a linear map of vector spaces $f : V \to W$, such that $f((T(g))(v)) = (S(g))(f(v))$, for all $g \in G$ and $v \in V$.

It is an *isomorphism* in case f is bijective.

Definition 3 (Module over a ring)**.** Consider a ring with unity, R, a commutative group $(M, +)$ together with an R-multiplication $R \times M \to M$ sending $(r, m) \in R \times M$ to $rm \in M$.

M is an R-module, if the R multiplication satisfies, for $r, r' \in R$ and $m, m' \in M$

$$(rr')m = r(r'm)$$

$$(r + r')m = rm + r'm$$

$$r(m + m') = rm + rm'$$

$$1m = m$$

Example 4. The group consisting of only one element, denoted by 0, is an R module with the R-multiplication $r0 = 0$.

Example 5. For any ring R, we may consider R as an R-module. The R-multiplication is the one inherited from the multiplication within R.

Definition 6 (Morphism of modules)**.** Let M and N be R-modules. A map $\varphi : M \to N$ is an *R-module homomorphism* if for $r \in R$ and $m, m' \in M$

$$\varphi(m + m') = \varphi(m) + \varphi(m')$$

$$\varphi(rm) = r\varphi(m))$$

Example 7. Given two modules M, N over a ring R, the *0-map* sending any $m \in M$ to $0_N \in N$ is an example of an R-homomorphism $M \to N$.

Definition 8 (Submodule)**.** A subset of an R-module M which, with the inherited operations, is again an R-module, is what we call a *submodule*.

Example 9 (Trivial submodules)**.** Given a ring R and an R-module N, we have always:

- N is an R-submodule of N;
- The identity element 0_N is an R-submodule of N.

Definition 10 (Simple module)**.** An R-module M different from 0 is called simple, if the only submodules of M are 0 and M.

Exercise 11. Given an R-module map $\varphi : M \to N$, show that the kernel ($\mathrm{Ker}\varphi = \{m \in M | \varphi(m) = 0_N \in N\}$) and the image ($\mathrm{Im}\varphi = \{\varphi(m) | m \in M\}$) are submodules of M and N respectively.

The group ring.

Definition 12 (Group ring)**.** Given a ring R and a group G, we may define the group ring RG as follows. The elements of the ring are of the form $\sum_{g \in G} r_g g$ where $\{r_g\}_{g \in G}$ are elements from R. Summation takes the following form:

$$\sum_{g \in G} r_g g + \sum_{g \in G} \rho_g g = \sum_{g \in G} (r_g + \rho_g) g,$$

where $(r_g + \rho_g)$ is the sum of r_g and ρ_g inside R.

Multiplication takes the form

$$\sum_{g \in G} r_g g \cdot \sum_{g' \in G} \rho_{g'} g' = \sum_{g \in G} \sum_{g' \in G} r_g \rho_{g'} g \cdot g'$$

which we may rewrite as

$$\sum_{g\in G} r_g g \cdot \sum_{g'\in G} \rho_{g'} g' = \sum_{x\in G} \left(\sum_{g\in G} (r_g \cdot \rho_{g^{-1}x}) g \right) x$$

Note 13. Any field is in particular a ring, so given a field, k, and a finite group G, we have defined the group ring kG.

Example 14 (Main example)**.** Given a finite group, G, an example of a group ring is $\mathbb{C}G$.

Example 15. From the ring $\mathbb{Z}/2$ and the group $G = \{e, g\}$ where $g^2 = e$, we may form the group ring $\mathbb{Z}/2G$. This group ring has only 4 elements:

$$0 \quad , \quad e \quad , \quad g \quad , \quad e + g,$$

all of which have order 2. We recognize this as $(\mathbb{Z}/2[x])/x^2$, or $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.

The $\mathbb{Z}/2$-representations of G are both one-dimensional, one is the identity, and the other sends g to -1.

The correspondence between $\mathbb{C}$-represenations of G and $\mathbb{C}G$-modules

We wish to go both directions: From a complex representation we want to form a $\mathbb{C}G$ module, and from a $\mathbb{C}G$-module we want to form a complex representation.

Proposition 16. *Given a representation $T : G \to \mathrm{End}_{\mathbb{C}}(V)$ of a finite group, G, we may form a module over the group ring $\mathbb{C}G$ as follows: Consider V as a commutative ring. Equip it with the $\mathbb{C}G$ action determined by*

$$gv = (T(g))(v).$$

Then this is a $\mathbb{C}G$-module.

Proof. There are four items to prove. Let $r, r' \in \mathbb{C}G$ and $v, v' \in V$

- $(rr')v = r(r'v)$: It is enough to check for $r, r' \in G$:

  $$(rr')v = (T(rr'))(v) = (T(r)T(r'))(v) = (T(r))(T(r')(v)) = T(r)(r'v) = r(r'v)$$

- $(r + r')v = rv + r'v$:

  $$\begin{aligned} \left(\textstyle\sum_{g\in G} r_g g + \sum_{g\in G} \rho_g g\right) v &= \left(\textstyle\sum_{g\in G} (r_g + \rho_g) g\right) v \\ &= \left(\textstyle\sum_{g\in G} (r_g + \rho_g) g v\right) \\ &= \left(\textstyle\sum_{g\in G} (r_g + \rho_g)(T(g))(v)\right) \\ &= \textstyle\sum_{g\in G} r_g (T(g))(v) + \sum_{g\in G} \rho_g (T(g))(v) \end{aligned}$$

- $r(v+v') = rv + rv'$: This is clear since for any endomorphism $\varphi \in \mathrm{End}_{\mathbb{C}}(V)$, we have $\varphi(v+v') = \varphi(v) + \varphi(v')$.
- $1v = v$: This holds since $T(1)$ is the identity endomorphism.

□

Proposition 17. *Given a module V over the group ring $\mathbb{C}G$ of a finite group G, we may form a complex representation of G as follows:*

Consider V as a complex vector field. We define $T : G \to \mathrm{End}_{\mathbb{C}}(V)$ such that T sends $g \in G$ to the endomorphism defined by $v \mapsto gv$.

Example 18. Given a group G, we may view $\mathbb{C}G$ as a $\mathbb{C}G$-module.

As a $\mathbb{C}$-vector space, $\mathbb{C}G$ is isomorphic to $\mathbb{C}^{|G|}$ with basis vectors $g \in G$. The G-action permutes the basisvectors as follows: $gh = g \cdot h$.

As a representation, this corresponds to the *regular* representation.

Not only does every complex representation correspond to a module over $\mathbb{C}G$, morphisms of representations correspond to morphisms of modules, direct sums correspond to direct sums and submodules correspond to invariant subspaces.

Proposition 19. *A $\mathbb{C}$-linear map $\varphi : V \to W$ is a morphism of complex G-representations if and only if it is a morphism of $\mathbb{C}G$-modules.*

Proof. Let V and W be $\mathbb{C}G$-modules, and let $\varphi : V \to W$ be a $\mathbb{C}$-linear map. Let V and W correspond to the representations $T : G \to \mathrm{End}_{\mathbb{C}}(V)$ and $S : G \to \mathrm{End}_{\mathbb{C}}(W)$, respectively.

Then $\varphi((T(g))(v)) = \varphi(gv)$ and $g\varphi(v) = (S(g))(\varphi(v))$, thus, $\varphi((T(g))(v)) = (S(g))(\varphi(v))$ if and only if $\varphi(gv) = g\varphi(v)$.

According to the definitions, the statement above is: φ is a morphism of $\mathbb{C}G$-modules if and only if φ is a morphism of G-representations. □

Note 20. Let $\varphi : V \to W$ be as above. Then φ is an isomorphism of $\mathbb{C}G$-modules if and only if it is an isomorphism of compex G-representations.

Proposition 21. *Let G be a finite group. Let V and W be the $\mathbb{C}G$-modules corresponding to the representations $T : G \to \mathrm{End}_{\mathbb{C}}(V)$ and $S : G \to \mathrm{End}_{\mathbb{C}}(W)$.*

Then the direct sum of modules, $V \oplus W$ corresponds to the direct sum of representations, $T \oplus S : G \to \mathrm{End}_{\mathbb{C}}(V \oplus W)$.

Proof. The direct sum of representations $T \oplus S$ corresponds to the $\mathbb{C}G$-module consisting of the commutative group $V \oplus W$ and the $\mathbb{C}G$-action that extends $g(v,w) = ((T \oplus S)(g))(v,w) = ((T(g))(v),(S(g))(w)) = (gv,gw) \in V \oplus W$ for $(v,w) \in V \oplus W$.

But then the $\mathbb{C}G$ action must satisfy, for $r \in \mathbb{C}G$, that $g(v,w) = (gv,gw)$. We recognize this as the direct sum $V \oplus W$ of $\mathbb{C}G$-modules. ☐

Proposition 22. *Given a finite group G and a complex representation $T : G \to \mathrm{End}_{\mathbb{C}}(V)$ of G.*

The G-invariant subspaces are exactly the $\mathbb{C}G$-submodules of V.

Proof. There are two implications to show.

- Let $U \subseteq V$ be a G-invariant subset of V. We wish to prove U is a $\mathbb{C}G$-submodule of V. We need to check $ru + u' \in U$, for $u, u' \in U$ and $r \in \mathbb{C}G$. It is enough to check $gu + u' \in U$ for $g \in G$. But $gu \in U$ since U is G-invariant, and then $gu + u' \in U$ simply because U is a vector space.
- Let $U \subseteq V$ be a $\mathbb{C}G$-submodule of V. We wish to prove U is a G-invariant subspace. Let $g \in G$ and $u \in U$, then $gu \in U$ since U is in particular a module. Hence, U is G-invariant.

☐

Corollary 23. *Simple modules correspond to irreducible representations*

Proof. Since submodules correspond to invariant subspaces, having only trivial submodules corresponds to having only trivial invariant subspaces. ☐

Properties of simple modules.

Proposition 24. *Simple modules are cyclic.*

Proof. Let $M \neq 0$ be a simple R-module. Since $M \neq 0$, choose $m \in M$, $m \neq 0$. Then $Rm = \{rm | r \in R\}$ is a submodule of M. Since $0 \neq 1m \in Rm$, $Rm \neq 0$. Therefore, since M is simple, Rm must equal M. ☐

Proposition 25. *Let R be a ring and let $M \neq 0$ and $N \neq 0$ be simple R-modules. Let $\varphi : M \to N$ be an R-homomorphism. Then φ is either 0 or an isomorphism.*

Proof. The kernel of φ is a submodule of M, and hence either 0 or M, since M is simple.

The image of φ is a submodule of N, and hence, since N is simple, the image $\mathrm{Im}\varphi$ is either 0 or N.

If the image is 0, we have the 0-homomorphism. If the image is N, the kernel is not M, and hence the kernel is 0. Now, since $\mathrm{Ker}\varphi = 0$ and φ is surjective, φ is an isomorphism. ☐

Corollary 26. *Let S and T be simple $\mathbb{C}G$-modules. If S is not isomorphic to T, then* $\mathrm{Hom}_{\mathbb{C}G}(S, T) \cong 0$.

Proof. Any homomorphism $\varphi : S \to T$ is either 0 or an isomorphism by (25). But by assumption, φ cannot be an isomorphism. Hence any $\varphi : S \to T$ must be 0. ☐

Proposition 27. *If S is a simple $\mathbb{C}G$–module then* $\mathrm{End}_{\mathbb{C}G}(S) \cong \mathbb{C}$ *as rings.*

Proof. As a $\mathbb{C}$–linear operator on S an element $\phi \in \mathrm{End}_{\mathbb{C}G}(S)$ has an eigenvalue λ, $\mathbb{C}$ being algebraically closed. The operator $\phi - \lambda I$ is singular as it maps an eigenvector corresponding to λ to zero. Now assuming S is finitely generated over $\mathbb{C}G$ and $|G|$ is finite, $\dim_{\mathbb{C}}(S)$ is finite so $\phi - \lambda I$ is not surjetive, since it is not injective. Now S is simple so $(\phi - \lambda I)S = 0$ implying $\phi - \lambda I = 0$ and every element in $\mathrm{End}_{\mathbb{C}G}(S)$ is of the form $\phi_c = cI$ for some $c \in \mathbb{C}$ (c clearly being determined uniquely by ϕ). Now the mapping

$$\theta\colon\ \mathrm{End}_{\mathbb{C}G}(S) \to \mathbb{C}$$

sending ϕ_c to c is an isomorphism of rings. ☐

When G is a finite group Maschkes theorem gives

Proposition 28. $\mathbb{C}G$ *is semisimple* $\mathbb{C}G$*–module.*

Proof. Let T_{reg} be the representation corresponding to $\mathbb{C}G$ under the correspondence between equivalence classes of irreducble finite–dimensional representations of G and isomorphism classes of finitely generated $\mathbb{C}G$–modules. By Maschke we can write T_{reg} as a direct sum of irreducible representations:

$$T_{reg} = n_1 T_1 \oplus \cdots \oplus n_s T_s$$

Now if M_i is the module corresponding to the representation T_i then, by (23), the T_i's are simple modules and the correspondence respects direct sums

$$\mathbb{C}G \cong n_1 M_1 \oplus \cdots \oplus n_s M_s \tag{1}$$

so $\mathbb{C}G$ is semisimple. □

Note 29. A reformulation of Maschke's theorem is, that kG is semisimple exactly when $|G|$ is invertible in k. Or in other words, exactly when $|G|$ and $\mathrm{char}(k)$ are coprime.

In the language of homological algebra, one may state, that kG is semisimple exactly when k is a projective kG-module. (A proof is found in [Iyengar04].)

We know from [Jøndrup06b] that each irreducible representation (modulo equivalence) occurs as a summand of the regular representation. This means that in the direct sum (1) each isomorphism class of simple $\mathbb{C}G$–modules is present. Also, the coefficients are given by $n_i = \dim T_i$, so in (1) the n_i's can be read off from the character table since $\dim T_i = \chi_i(1)$.

Bibliography

[Foxby04] Hans-Bjørn Foxby, *Homological algebra*, 2004, lecture notes.
http://www.math.ku.dk/ma/kurser/mat4ha/ha.pdf

[Iyengar04] Srikanth Iyengar, *Modules and cohomology over group algebras: One commutative algebraist's perspective. Trends in commutative algebra*, 2004.

[Jøndrup06a] Søren Jøndrup, *Complex representations of finite groups*, 2006, lecture notes.

[Jøndrup06b] Søren Jøndrup, *Complex representations of finite groups ii*, 2006, lecture notes.