A BRIEF SUMMARY OF MODULAR REPRESENTATION THEORY

ROBERT PRAG

Abstract. This paper shall provide a brief summary of representation theory, with a focus on how the semi-simple case differs from the modular case. It will be assumed that the reader has a reasonable background in algebra, but not assuming an existing understand of representation theory.

Contents

1. Basic terminology

Let F be a field of characteristic p, and let V be an F vector space. Let G be a finite group of order n.

Definition 1.1. Then we define a *linear G representation of V over F* as a homomorphism $\phi : G \to GL(V)$.

Definition 1.2. We say the representation is *faithful* if ϕ is injective.

There is a bijection between $FG-$modules and pairs (V, ϕ).

Definition 1.3. Representations are *similar* or *equivalent* if they correspond to isomorphic FG-modules, otherwise they are *inequivalent.*

Definition 1.4. A module M is *irreducilbe* or *simple* if the only submodules are M and 0. If not, M is *reducible.*

Definition 1.5. M is *decomposible* if there exist nonzero submodules M_1 and M_2 such that $M = M_1 \oplus M_2$, otherwise it is *indecomposible.*

Definition 1.6. M is *completely reducible* if it can be written as the direct sum of irreducible submodules.

Date: August 17, 2007.

A representation inherits any of the above properties if the corresponding FG-module has the property with the same name.

Throughout this paper, many proofs will be cited rather than copied. This is not to force the reader to go find copies of the texts cited, merely to inform the reader of the validity of the statement without having to focus on it for the full of its proof. Also, in many cases proofs were cited because they used many other things which their author had already proven which I have not (as representation theory is complicated, it is unlikely that useful facts on it will appear without many other facts before them).

2. A handful of Exmples

Example 2.1. Let $G = \mathbb{Z}_6$ and let $V = \mathbb{Q}^3$. Let z be a generator for G. It suffices to define the representation by defining where it maps z. Define a homomorphism $\phi : \mathbb{Z}_6 \to GL_3(\mathbb{Q})$ such that

$$\phi : z \mapsto \begin{pmatrix} 0 & \frac{-1}{2} & 0 \\ 0 & 0 & -2 \\ -1 & 0 & 0 \end{pmatrix}$$

Which defines a representation (z^6 is the identity, and so is $(\phi(z))^6$. The kernel of ϕ is trivial here, although it need not be. Therefore the representation is faithful.

Example 2.2. Let $G = (\mathbb{H}, \times)$ and let $V = \mathbb{R}$. Define $\phi : G \to GL(\mathbb{R})$ by $\phi(x) = |x|$ i.e. multiplication by the norm of x. This is a representation, and this certainly has a non-trivial kernel.

Example 2.3. There is always the trivial representation: Let G be any group and let V be any vector space over any field F. Then $\phi : G \to GL_F(V)$ defined by $\forall g \in G, \phi(g) = id_V$ is a representation.

Example 2.4. Here's a modular representation: $F = \mathbb{F}_5, G = \mathbb{Z}_{20}$ and let a be a generator for G. Take V to be a one dimensional vector space over F. Define a homomorphism $\phi : G \to GL_F(V)$ by $\forall v \in V, \phi(a)v = 2v$. This defines a representation (because $2^{20} \mod 5 = 1$). Note, however, that every element of order five ($\{a^4, a^8, a^{12}, a^{16}\}$) acts trivially on V.

Example 2.5. Here is one more non-modular representation: Let $G = D_8$ and let $V = {\mathbb{F}_5}^2$. Define ϕ by

$$\phi(r) = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \phi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This defines a two dimensional representation of G.

3. Maschke's Theorem

Theorem 3.1 (Maschke)**.** *Let G be a finite group and let F be a field of characteristic p such that $p \not| \, |G|$. If V is any FG-module and U is any submodule of V, then there exists W a submodule of V such that $U \oplus W = V$.*

Proof. [2] (p. 849) The proof depends on the characteristic of the field not dividing the order of the group. □

This is a particularly useful result, and one that we would hope *in general.* However, in the modular case (that is, if p divides the order of G) then this result isn't true. In fact for any group there will be at least one counter-example.

Example 3.2. The regular representation of a cyclic group of order p^α is indecomposable.

Proof. [1] Let G be the cyclic group of order p^α and let a be a generator of G, let F be a field of characteristic p. Let M be any F-representation of G given by $\sigma : g \to Aut(M)$. Then $a_0 = \sigma(a)$ has the property that $1 = {a_0}^{p^\alpha}$. From this we may conclue that the minimal polynomial of a_0 divides $(x-1)^{p^\alpha}$. This implies that the only eigenvalue of a_0 is one, and thus M contains the one-dimensional trivial representation τ. Thus τ is the only irreducible representation of G. By writing the matrix for a_0 in Jordan block form we see that M is indecomposable iff there is a single Jordan block. Thus we have one (unique up to isomorphism) indecomposable representation of M with dimension s for each $1 \leq s \leq p^\alpha$. In particular, $F(G)$ is indecomposable. □

Lemma 3.3. [1] *Let G be a p-group and let F be as above. Then FG is indecomposable.*

Proof. Claim τ is the only irreducible representation of G, and that $F(G)$ is indecomposable as an $F(G)$-module. We prove the first claim by induction on n. Let $\sigma\colon G \to Aut(M)$ be any F-representation of G. If G is cyclic, then by [above] we are done. If not, let H be a cyclic subgroup of the center of G, generated by an element h. ... Let M_0 be the largest subspace of M on which H acts trivially. Again [as above], $M_0 \neq \{0\}$. As H is central, M_0 is a subrepresentation of M. But then the action of G on M_0 factors through the quotient G/H, so, by induction, τ is a subrepresentation of M_0 as a representation of G/H, and hence also as a representation of G. As for the second claim, if $F(G)$ were decomposable, say $F(G) = M_1 \oplus M_2$, then each of M_1 and M_2 would contain τ as a subrepresentation, so $F(G)$ would contain $\tau \oplus \tau$ as a subrepresentation. But it is easy to check that the subspace of $F(G)$ fixed by every element of G consists exactly of the multiples of $\Sigma_{g\in G} g$, which is 1-dimensional, a contradiction. □

Perhaps more problematically, these two results imply the following, which will show us that we are very unlikely to get to use anything that we can do in the semi-simple case, and therefore the modular case is going to be very different if we can prove anything about it.

Theorem 3.4. *Let G be a group of order $q \cdot p^a$ such that $gcd(p, q) = 1$. Let F be a field of characteristic p. Then G possesses finitely generated FG-modules which are completely reducible.*

Proof. [2] FG as a left FG-module is not completely reducible. □

As the theorem above should make clear, it is very much not a reasonable strategy to attempt to get information about a modular representation just by trying to decompose it into simple modules. This is a useful technique for determining the behavior of a semi-simple representation, as they decompose into a unique sum of simple modules. One would hope to find a way to get a modular representation to do something similarly nice. Before further investigating the modular case, I am going to present a few very powerful consequences of Maschke's theorem, to make it clear how nice semi-simple representations are.

4. Consequences in the semi-simple case

Theorem 4.1. *If $|G|$ is finite and $char(F) \not| \ |G|$ then every finitely generated FG-module is completely reducible.*

Proof. [2]Let V be the vector space corresponding to such a module. Then V is finite dimensional. Induct on $dim(V)$: If $dim(V) = 0$ or 1 then there is nothing to prove. If $dim(V) = 2$ Maschke's theorem tells us that the module U corresponding to any one dimensional subspace has W a non-zero sub-module of V such that $V = U \oplus W$. If $dim(V) = n$ then Maschke's theorem tells us that the corresponding module is the direct sum of two completely reducible modules, and is thus completely reducible. □

Definition 4.2. A module P over a ring R is projective if it is a direct summand of a free R-module.

Definition 4.3. A module Q over a ring R is injective if whenever Q is a submodule of an R-module M, Q is a direct summand of M.

Theorem 4.4 (Artin-Wedderburn)**.** *The following are equivalent*

(1) every R-module is projective
(2) every R-module is injective
(3) every R-module is completely reducible
(4) the ring R considered as a left R-module is a direct sum of simple modules L_i of the form $L_i = Re_i$ such that $e_ie_j = 0$ if $i \neq j$, ${e_i}^2 = e_i$ and $\Sigma^n{}_{i=1}e_i = 1$.
(5) as rings, R is isomorphic to a direct product of matrix rings over division rings.

Proof. That (1) and (2) are equivalent is a matter of definition checking. That (3) implies (2) is a result of trying to take a maximal submodule that does not contain Q and deducing that this must be a direct summand of Q. That (4) implies (3) relies on taking direct sums of simple sub-modules and using choice to show that the maximal such sum must be the full module. That (5) implies (4) and that (2) implies (5), as well as the details of the others, may be looked up [2], p. 863. □

This is an extremely powerful result, and classifies semi-simple representations, reducing the remaining questions in that field to much simpler questions about simple modules. Further, it garentees a decent amount about a module, which makes it much easier to work with. However, it is very clear that no such result could apply in the modular case, as the existance of such a decomposition into semi-simple modules would imply the result of Maschke's Theorem, a result which has been explicitly proven only to apply in the semi-simple case.

5. An explicit computation

In an attempt to evaluate the viability of carrying over the methods and strategies used for semi-simple representations, I have included a composition series for a modular representation. Let $F = \mathbb{F}_2$ be a field of characteristic two. Call the generators for $D_8 = \langle r, s\rangle$ such that $r^4 = s^2 = e$.

Note the following composition series:

$$0 \subset \left\langle 1 + r + r^2 + r^3 + s + sr + sr^2 + sr^3 \right\rangle \subset \left\langle 1 + r + r^2 + r^3, s + sr + sr^2 + sr^3 \right\rangle$$

$$\subset \left\langle 1 + r^2 + s + sr^2, 1 + r + r^2 + r^3, s + sr + sr^2 + sr^3 \right\rangle$$

$$\subset \left\langle 1 + r^2, s + sr^2, 1 + r + r^2 + r^3, s + sr + sr^2 + sr^3 \right\rangle$$

$$\subset \left\langle 1 + s, 1 + r^2, s + sr^2, 1 + r + r^2 + r^3, s + sr + sr^2 + sr^3 \right\rangle$$

$$\subset \left\langle 1 + r, 1 + s, 1 + r^2, s + sr^2, 1 + r + r^2 + r^3, s + sr + sr^2 + sr^3 \right\rangle$$

$$\subset \left\langle 1 + r, 1 + r^2, 1 + r^3, 1 + s, 1 + sr, 1 + sr^2, 1 + sr^3 \right\rangle \subset D_8$$

This shows that D_8 is reducible, but it does not show that it is decomposable. A similar computation on $F\mathbb{Z}_8$ will also produce such a composition series, indicating that it is also reducible. However, neither of these modules is decomposable, as they would each decompose to $\tau \oplus \tau \oplus \tau \oplus \tau \oplus \tau \oplus \tau \oplus \tau \oplus \tau$, as τ, the trivial representation, is the only only one-dimensional modular representation.

With this in mind, we will clearly need to look at something other than simple submodules if we wish to make any progress toward understand modular representations.

6. Some tools for dealing with modular representations

Definition 6.1. Let R be a ring. Then the **Jacobson radical** $J = J(R)$ is the intersection of all the maximal left ideals of R.

Lemma 6.2. *$J(R) = \cap Ann(M)$ taken over all simple left R-modules M.*

Proof. [1]Let $y \in$Ann(M). Let I be a maximal ideal. Then R/I is a simple left R-module, so $y(R/I) = 0$, so $y \in I$ and therefore $y \in J(R)$. Suppose $x \in J(R)$ and let M be any simple left R-module. Because M is simple, it must be cyclic and generted by any non-zero element m. Thus $M \cong R/$Ann(m). Since M is simple, Ann(m) is a maximal ideal. Thus $x \in$Ann(m), and thus $x \in \cap_{m\in M} = Ann(M)$. □

As a result of this lemma, it is clear that the choice of left ideals instead of right ideals made no difference.

Definition 6.3. Define a ring R to be $J - semisimple$ if $J(R) = 0$.

Proposition 6.4.

(1) Let R be an $\mathbb{F}_p$-algebra, let F be an arbitrary field of characteristic p, and let $R' = F \otimes_{\mathbb{F}_p} R$. Then $J(R') \supseteq F \otimes_{\mathbb{F}_p} J(R)$.

(2) If R is a finite-dimensional $\mathbb{F}_p$-algebra, then $J(R') = F \otimes_{\mathbb{F}_p} J(R)$, and hence $R'/J(R') \cong F \otimes_{\mathbb{F}_p} (R/J(R))$.

Proof. (1) [1] $J(R)$ is a nilpotent ideal in R, and hence $F \otimes_{\mathbb{F}_p} J(R)$ is a nilpotent ideal in R', so $F \otimes_{\mathbb{F}_p} J(R) \subseteq J(R')$.

(2) [1] p. 181. □

Theorem 6.5. *Let R be a finite-dimensional algebra over an algebraically closed field F. Then there are only finitely many simple R-modules, up to isomorphism. If their degrees are $\{d_i\}$ then*

$$\Sigma {d_i}^2 = \dim_F R - \dim_F J(R)$$

Proof. [1] p. 183. The proof is based on $R/J(R)$ being semi-simple. □

Lemma 6.6. *Let R be a ring of finite length. Then $J(R)$ is the largest nilpotent left ideal in R.*

Proof. [1]. □

7. Results for Modular Representations

Let G be a finite group of order np^a, such that p is prime and p does not divide n. Let P be a Sylow p-subgroup of G.

Lemma 7.1. *Let V be a simple $F(G)-$module and let H be any normal p-subgroup of G. Then H acts trivially on V.*

Proof. [1] (p. 188). Proof works by finding a semi-simple $F(H)$-module as a subset, and showing that must be trivial.

□

Theorem 7.2 (Wallace)**.** *: Let $R = F(G)$ where G is a p-group. Then $J(R) = \mathscr{R}_0$, the augmentation ideal of R, and* $\dim_F J(R) = p^a - 1$.

Proof. [1] $\dim_F \mathscr{R}_0 = p^a - 1$. $\mathscr{R}_0$ is a maximal left ideal, and therefore $J(R) \subseteq (R)_0$. However, $\dim_F R - \dim_{J(R)} = 1$ by Theorem 6.5. Thus $J(R) = \mathscr{R}_0$ □

Theorem 7.3. *Suppose that P is a normal subgroup of G and let $R = F(G)$. Then $J(R)$ is the ideal generated by $J(F(P))$ (under the natural inclusion of $F(P)$ in $F(G)$), and* $\dim_F J(R) = n(p^a - 1)$.

Proof. $\mathscr{R}_0$ is generated by $\{g - 1 | g \in G\}$. Wallace's theorem shows that when $G = P$, $J(F(P))$ is generated by $\{b - 1 | b \in P\}$ which implies that $\dim_F RJ(F(P)) = n(p^a - 1)$. Take $g_1, g_2 \in G, b_1, b_2 \in P, g_1(b_1 - 1)g_2(b_2 - 1) = g_1 g_2(b_1' - 1)(b_2 - 1)$ where $b_1' = g_2^{-1} b_1 g_2 \in P$ because P is normal. Further, we see that $J(F(P))$ is nilpotent, so we have that $RJ(F(P))$ is nilpotent as well. Hence $RJ(F(P)) \subseteq J(R)$. For the rest of this proof, please see [1]. □

A very similar argument also proves the following:

Theorem 7.4. *Let H be any normal p-subgroup of G. Then $J(R)$ contains the ideal generated by $J(F(H))$. In particular, this holds when H is the intersection of all the p-Sylow subgroups of G.*

Lemma 7.5. *For any prime p, any $g \in G$ can be expressed uniquely as $g = ab$ such that p does not divide the order of a and the order b is a power of p, and $ab = ba$. In this situation, both a and b are powers of g.*

Proof. [1]Let $n = |g|$. If $(n, p) = 1$, the proof is trivial. If $n = p^r q$ with $r \geq 1$ and $(p, q) = 1$ then set $1 = xp^r + yq$ for some integers x and y. Set $a = g^{xp^r}$ and $b = g^{yq}$. □

Definition 7.6. Define a, b as above. a is called the p-regular factor, and b is called the p-singular factor. If $b = 1$ i.e. $|g|$ is prime to p, g is called a p-regular element. If $a = 1$ i.e. $|g|$ is a power of p, then g is called a p-singular element.

Corollary 7.7. *Let F be algebraically closed. Let V be an F-representation of G, given by $\sigma : G \rightarrow Aut(V)$. Let g be an element of G and write $g = ab$ as in Lemma 7.5. Then the eigenvalues of $\sigma(g)$ and $\sigma(b)$ are the same with the same multiplicity.*

Proof. [1]Chose a basis in which $\sigma(g)$ is in Jordan canonical form. Since a and b are powers of g, $\sigma(a)$ and $\sigma(b)$ are upper triangular, and since the order of a is a power of p, the diagonal entries of $\sigma(a)$ are all 1. But $\sigma(g) = \sigma(a)\sigma(b)$. □

Theorem 7.8 (Brauer-Nesbitt)**.** *Let V_1 and V_2 be semi-simple F-representations of G, where F is algebraically closed, given by $\sigma_i : G \rightarrow Aut(V_i), i = 1, 2$. Then V_1 and V_2 are isomorphic iff $\sigma_1(g)$ and $\sigma_2(g)$ have the same characteristic polynomials or, equivalently, the same eigenvalues with the same multiplicities, for every g in G.*

Proof. [1] (p. 194). □

Definition 7.9. Chose an isomophism α from the group of q-th roots of unity in F to the group of q-th roots of unity in $\mathbb{C}$. Let V be an F-representation of G given by $\sigma : G \rightarrow Aut(V)$. The Brauer character β_V is the complex-valued class function on p-regular elements of G defined as follows. If $\{x_i\}$ are the eigenvalues of $\sigma(g)$ (each of which is a $q - th$ root of 1 in F) with multiplicities, then

$$\beta_V(g) = \Sigma\alpha(x_i)$$

Theorem 7.10 (Brauer-Nesbitt)**.** *. Let V_1 and V_2 be F-representations of G, where F is a splitting field for G. Then V_1 and V_2 have the same irreducible components with the same multiplicities, iff $\beta_{V_1}(g) = \beta_{V_2}(g)$ for every p-regular element of G.*

Proof. [1] The only-if part should be trivial. Observe that for any F-representation V of G, if $\beta_V(g) = \Sigma\alpha(x_i)$ per the definition of the Brauer character, then $\beta_V(g^r) = \Sigma\alpha({x_i}^r) = \Sigma\alpha(x_i)^r$ for every r, so, by considering the elementary symmetric polynomials in $\{\alpha(x_i)\}$, we can derive that $\{\beta_V(g^r)|r = 1, 2, ...\}$ determines $\{\alpha(x_i)\}$, and hence $\{x_i\}$, and then the theorem follows from Lemma 7.7 and Theorem 7.8. □

The Brauer-Nesbitt theorem is a substantial improvement, as we now have both a useful tool for studying modular representations and an easy way to verify if two modular representations have the same irreducible components. While it is unfortunate that we don't get anything nearly so powerful as Maschke's theorem, we still can know a fair amount about modular representations from Brauer characters.

References

[1] Steven H. Wientraub. Representation Theory of Finite Groups: Algebra and Arithmetic. American Mathematical Society, 2003

[2] David S. Dummit and Richard M. Foote. Abstract Algebra. John Wiley and Sons, Inc., 2004