

UNIVERSITY OF MISSOURI

MASTER'S PROJECT

A Survey on Character Tables for Representations of Finite Groups

Author:
Jared Stewart

Supervisor:
Dr. Calin Chindris

*A project submitted in fulfilment of the requirements
for the degree of Masters of Arts
in the*

Department of Mathematics

January 16, 2016

Acknowledgements

The acknowledgements and the people to thank go here, don't forget to include Professor Chindris...

Contents

Acknowledgements	iii
1 Basic Notions of Representation Theory	1
1.1 Group Actions	1
1.2 The Definition of a Representation	2
1.3 Representations of Cyclic Groups	4
1.4 Constructions from Linear Algebra	6
1.5 Complete Reducibility and Unitarity	6
Bibliography	9

Chapter 1

Basic Notions of Representation Theory

1.1 Group Actions

Definition 1.1. A *(left) group action* of a group G on a set X is a map $\varphi: G \times X \rightarrow X$ (written as $g \cdot a$, for all $g \in G$ and $a \in A$) that satisfies the following two axioms:

$$1 \cdot x = x \quad \forall x \in X \quad (1.1.1)$$

$$(gh) \cdot x = g \cdot (h \cdot x) \quad \forall g, h \in G, x \in X \quad (1.1.2)$$

Note. We could likewise define the concept of a *right* group action, where the set elements would be multiplied by group elements on the right instead of on the left. Throughout we shall use the term *group action* to mean a *left* group action.

Proposition 1.2. Let G act on the set X . For any fixed $g \in G$, the map σ_g from X into X defined by $\sigma_g(x) = g \cdot x$ is a permutation of the set X , i.e. $\sigma_g \in S_X$.

Proof. We show that σ_g is a permutation of X by finding a two-sided inverse map, namely $\sigma_{g^{-1}}$. Observe that for any $x \in X$, we have

$$\begin{aligned} (\sigma_{g^{-1}} \circ \sigma_g)(x) &= \sigma_{g^{-1}}(\sigma_g(x)) && \text{(by definition of function composition)} \\ &= g^{-1} \cdot (g \cdot x) && \text{(by definition of } \sigma_g \text{ and } \sigma_{g^{-1}}) \\ &= (g^{-1}g) \cdot x && \text{(by axiom 1.1.1 of an action)} \\ &= 1 \cdot x \\ &= x && \text{(by axiom 1.1.2 of an action).} \end{aligned}$$

Thus $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map on X . We can reverse the roles of g and g^{-1} to see that $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map on X . Having a two-sided inverse, we conclude that σ_g is a permutation of X . \square

Proposition 1.3. Let G act on the set X . The map from G to the symmetric group S_X defined by $g \mapsto \sigma_g(x) = g \cdot x$ is a group homomorphism.

Proof. Define the map $\varphi: G \rightarrow S_X$ by $\varphi(g) = \sigma_g$. We have seen from Proposition 1.2 that σ_g is indeed an element of S_X . It remains to show that $\varphi(g_1g_2) = \varphi(g_1) \circ \varphi(g_2)$ for any $g_1, g_2 \in G$. Observe that

$$\begin{aligned}
\varphi(g_1 g_2)(x) &= \sigma_{g_1 g_2}(x) && \text{(by definition of } \varphi) \\
&= (g_1 g_2) \cdot x && \text{(by definition of } \sigma_{g_1 g_2}) \\
&= g_1 \cdot (g_2 \cdot x) && \text{(by axiom 1.1.1 of an action)} \\
&= \sigma_{g_1}(\sigma_{g_2}(x)) && \text{(by definition of } \sigma_{g_1} \text{ and } \sigma_{g_2}) \\
&= \varphi(g_1)(\varphi(g_2)(x)) && \text{(by definition of } \varphi) \\
&= (\varphi(g_1) \circ \varphi(g_2))(x) && \text{(by definition of function composition).}
\end{aligned}$$

Since the values of $\varphi(g_1 g_2)$ and $\varphi(g_1) \circ \varphi(g_2)$ agree on every element $x \in X$, these two permutations are equal. We conclude that φ is a homomorphism, since g_1 and g_2 were arbitrary elements of G . \square

Proposition 1.4. *Any homomorphism ψ from the group G into the symmetric group on S_X on a set X gives rise to an action of G on X , defined by taking $g \cdot x = \psi(g)(x)$.*

Proof. Suppose that we have a homomorphism ψ from G into S_X . We can define a map from $G \times X$ to X by $g \cdot x = \psi(g)(x)$. We verify that this map satisfies the definition of a group action of G on X :

$$\text{(axiom 1.1.1)} \quad 1 \cdot x = \psi(1)(x) = id_X(x) = x$$

$$\text{(axiom 1.1.2)} \quad (gh) \cdot x = \psi(gh)(x) = (\psi(g)\psi(h))(x) = \psi(g)(\psi(h)(x)) = g \cdot (h \cdot x) \quad \square$$

Proposition 1.5. *The actions of G on the set X are in bijective correspondence with the homomorphisms from G into the symmetric group S_X .*

Proof. By Proposition 1.3, any action of G on X yields a homomorphism from G into S_X . Conversely, any homomorphism from G into S_X establishes an action of G on X by Proposition 1.4. \square

1.2 The Definition of a Representation

Definition 1.6. Let G be a group, let F be a field, and let V be a vector space over F . A **linear representation** of G is any group homomorphism $\varphi: G \rightarrow GL(V)$.

Definition 1.7. Let G be a group, let F be a field, and let V be a vector space over F . A **linear representation** of G is any action of G on V which preserves the linear structure of V , that is,

$$g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2 \quad \forall g \in G, v_1, v_2 \in V \quad (1.7.1)$$

$$g \cdot (kv) = k(g \cdot v) \quad \forall g \in G, v \in V, k \in F \quad (1.7.2)$$

Note. Unless otherwise specified, we use *representation* to mean *finite-dimensional complex representation*.

Proposition 1.8. *The definitions of a linear representation given in 1.6 and 1.7 above are equivalent.*

Proof. (\rightarrow) Suppose that we have a homomorphism $\varphi: G \rightarrow GL(V)$. Note that $GL(V)$ is a subgroup of the symmetric group S_V on V , so we can apply Proposition 1.4 to obtain an action of G on V by $g \cdot v = \varphi(g)(v)$. We check that this action preserves the linear structure of V .

1.7.1 For any $g \in G, v_1, v_2 \in V$ we have $g \cdot (v_1 + v_2) = \varphi(g)(v_1 + v_2) = \varphi(g)(v_1) + \varphi(g)(v_2) = g \cdot v_1 + g \cdot v_2$.

1.7.2 For any $g \in G, v \in V, k \in F$ we have $g \cdot (kv) = \varphi(g)(kv) = k(\varphi(g)(v)) = k(g \cdot v)$.

- (\Leftarrow) Suppose that we have an action of G on V which preserves the linear structure of V in the sense of Definition 1.7. We can apply Proposition 1.3 to obtain a homomorphism $\varphi: G \rightarrow S_V$ given by $\varphi(g) = \sigma_g$ where $\sigma_g(v) = g \cdot v$. It remains to show that the image $\varphi(G)$ of G under φ is actually contained in $GL(V)$, i.e. that for each $g \in G$ the map σ_g is linear. Fix an element $g \in G$. For any $k \in F$ and $v \in V$ we have

$$\begin{aligned} \sigma_g(kv) &= g \cdot (kv) && \text{(by definition of } \sigma_g) \\ &= k(g \cdot v) && \text{(by property 1.7.1)} \\ &= k(\sigma_g(v)) && \text{(by definition of } \sigma_g). \end{aligned}$$

Also, for any $v_1, v_2 \in V$ we have

$$\begin{aligned} \sigma_g(v_1 + v_2) &= g \cdot (v_1 + v_2) && \text{(by definition of } \sigma_g) \\ &= g \cdot v_1 + g \cdot v_2 && \text{(by property 1.7.2)} \\ &= \sigma_g(v_1) + \sigma_g(v_2) && \text{(by definition of } \sigma_g). \end{aligned}$$

Thus σ_g is linear, and $\varphi(G) \subset GL(V)$ proves that we have a homomorphism $\varphi: G \rightarrow GL(V)$. □

Definition 1.9. Let G be a group, let F be a field, let V be a vector space over F , and let $\varphi: G \rightarrow GL(V)$ be a representation of G . The **dimension** of the representation is the dimension of V over F .

- Example 1.10.** 1. Let V be a 1-dimensional vector space over the field F . The map $\varphi: G \rightarrow GL(V)$ defined by $\varphi(g) = 1$ for all $g \in G$ is a representation called the *trivial representation* of G . The trivial representation has dimension 1.
2. If a finite group G acts on a finite set X and F is any field, then there is an associated *permutation representation* on the vector space V over F with basis $\{e_x: x \in X\}$. We let G act on the basis elements by $g \cdot e_x = e_{gx}$ for all $x \in X$ and $g \in G$. Note that G permutes the basis elements of V .
3. A fundamental special case of a permutation representation is given by a finite group acting on itself by left multiplication. In this case, the elements of G form a basis for V , and each $g \in G$ permutes the basis elements by $g \cdot g_i = gg_i$. This is called the *regular representation* of G and has dimension $|G|$. We shall see later that this representation encodes information about all other representations of G .
4. For any symmetric group S_n the *alternating representation* on $V = \mathbb{C}$ is given by the map $\varphi: S_n \rightarrow GL(\mathbb{C}) = \mathbb{C}^\times$ defined by $\varphi(\sigma) = \text{sgn}(\sigma)$. More generally, for any group G with a subgroup H of index 2, we can define an *alternating representation* $\varphi: G \rightarrow GL(\mathbb{C})$ by letting $\varphi(g) = 1$ if $g \in H$ and $\varphi(g) = -1$ if $g \notin H$. (We recover our original example by taking $G = S_n$ and $H = A_n$.)

Definition 1.11. A **homomorphism** between two representations $\varphi_1: G \rightarrow GL(V)$ and $\varphi_2: G \rightarrow GL(W)$ is a linear map $\psi: V \rightarrow W$ that intertwines with (respects) the G -action, i.e. such that

$$\psi(\varphi_1(g)(v)) = \varphi_2(g)(\psi(v)) \quad \forall v \in V, g \in G$$

An **isomorphism** of representations is a homomorphism of representations that is also an invertible map.

Note. If we have representations (φ_1, V) and (φ_2, W) and an isomorphism of vector spaces $\psi: V \rightarrow W$ then we can rewrite the compatibility requirement above as $\varphi_2(g) = \psi \circ \varphi_1(g) \circ \psi^{-1}$ for all $g \in G$.

Given any representation (φ, V) of G on a vector space V over a field F of dimension n , we can fix a basis for V to obtain an isomorphism of vector spaces $\psi: V \rightarrow F^n$. We obtain a representation ϕ of G on F^n by defining $\phi = \psi \circ \varphi(g) \circ \psi^{-1}$ for all $g \in G$. Clearly, this representation is isomorphic to the original representation (φ, V) . In particular we can always choose to view n -dimensional complex representations as representations on \mathbb{C}^n where each $\phi(g)$ is given by an $n \times n$ matrix with entries in \mathbb{C} .

Suppose that we have two representations $\varphi: G \rightarrow GL_n(F)$ and $\phi: G \rightarrow GL_m(F)$ given by $\varphi(g) = X_g$ and $\phi(g) = Y_g$. A homomorphism between these representations is then an $m \times n$ matrix A such that $AX_g = Y_gA$ for all $g \in G$. An isomorphism is given precisely when such A is square and invertible. Thus, two representations $\varphi: G \rightarrow GL_n(F)$ and $\phi: G \rightarrow GL_n(F)$ are isomorphic if and only if there exists $A \in GL_n(F)$ such that $\varphi(g) = A\phi(g)A^{-1}$ for all $g \in G$. This establishes the following proposition:

Proposition 1.12. *The isomorphism classes of n -dimensional representations of G on \mathbb{C} are in bijection with the quotient $Hom(G; GL_n(\mathbb{C}))/GL_n(\mathbb{C})$ of group homomorphisms $G \rightarrow GL_n(\mathbb{C})$ modulo the conjugation action of $GL_n(\mathbb{C})$.*

1.3 Representations of Cyclic Groups

Example 1.13 (Representations of \mathbb{Z}). We want to classify all representations of the group \mathbb{Z} under addition. Consider an n -dimensional representation $\varphi: \mathbb{Z} \rightarrow GL_n$. For φ to be a group homomorphism requires that $\varphi(0) = \text{Id}$. Observe that for any $0 \neq n \in \mathbb{Z}$, we have $\varphi(n) = \varphi(1 + \dots + 1) = \varphi(1)^n$. Thus φ is completely determined by the matrix $\varphi(1) \in GL_n(\mathbb{C})$, and any such matrix determines a representation of \mathbb{Z} . It follows that the n -dimensional isomorphism classes of representations of \mathbb{Z} are in bijection with the conjugacy classes in $GL_n(\mathbb{C})$. These conjugacy classes can be parameterized by the *Jordan canonical form*.

Example 1.14 (Representations of the cyclic group of order n). We shall classify all representations of the cyclic group $G = 1 = g^n, g, \dots, g^{n-1}$ of order n . Consider a representation $\varphi: G \rightarrow GL(V)$. As in the previous example, we know that $\varphi(1) = \text{Id}$ and $\varphi(g^k) = \varphi(g)^k$. Thus our representation φ is determined completely by the linear transformation $\varphi(g)$. It will be helpful to fix a basis of V so that we may view $\varphi(g)$ as a matrix A . Recall from linear algebra that there exists a basis in which $\varphi(g)$ takes the *Jordan normal form*.

$$A = \begin{bmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_m \end{bmatrix}$$

where each *Jordan block* J_k takes the form

$$J_k = \begin{bmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \ddots & 0 & 0 \\ 0 & 0 & \lambda & \ddots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 1 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{bmatrix}.$$

Now $I = A^n$ is a block-diagonal matrix with diagonal blocks J_k^n , so we must have that each block $J_k^n = \text{Id}$. Observe that we can write each block as $J_k = \lambda \text{Id} + N$ where N is the Jordan block with $\lambda = 0$. Thus we have

$$\text{Id} = J_k^n = (\lambda \text{Id} + N)^n = \lambda^n \text{Id} + \binom{n}{1} \lambda^{n-1} N + \binom{n}{2} \lambda^{n-2} N^2 + \dots + \binom{n}{n-1} \lambda N^{n-1} + N^n$$

.

Lemma 1.15. *Let N be the Jordan block with $\lambda = 0$ of size $n \times n$. For any integer p with $1 \leq p \leq n-1$, then N^p is the matrix with ones in the positions (i, j) where $j = i + p$ and zeroes everywhere else. (The ones lie along a line parallel to the diagonal, p steps above it.)*

Proof. (By induction.)

- *Base case* This is simply the definition of N .
- *Inductive step* Suppose that the lemma holds for N^p . We compute the (i, j) entry of N^{p+1} :

$$(N^{p+1})_{i,j} = \sum_{k=1}^n (N^p)_{i,k} N_{k,j} = (N^p)_{i,i+p} N_{i+p,j} = N_{i+p,j} = \begin{cases} 1 & \text{if } j = i + (p+1) \\ 0 & \text{otherwise} \end{cases}$$

□

Now, if $N \neq 0$ then each term $\binom{n}{k} \lambda^{n-k} N^k$ for $k > 0$ would yield some non-zero non-diagonal entries (in the positions (i, j) where $j = i + k$) and hence our sum could not equal the identity matrix. We must conclude that $N = 0$, and $J_k = \lambda^n$ is a 1×1 block. Thus $\varphi(g)$ is a diagonal matrix with n th roots of unity as diagonal entries.

To summarize, every m -dimensional representation φ of the cyclic group $G = \langle g \rangle$ of order n can be seen to act (in the right choice of basis) as $m \times m$ diagonal matrices with n th roots of unity along the diagonal. In particular, these representations are determined completely by the value of $\varphi(g)$ and are classified up to isomorphism by unordered m -tuples of n th roots of unity.

1.4 Constructions from Linear Algebra

Definition 1.16. A **subrepresentation** of V is a G -invariant subspace $W \subseteq V$; that is a subspace $W \subseteq V$ with the property that $\varphi(g)(w) \in W$ for all $g \in G, w \in W$. Note that W effects a representation of G under the action $\varphi(g)|_W$.

From elementary linear algebra, we know that given a subspace $W \subseteq V$, we can form the **quotient space** V/W consisting of cosets $v + W$ in V . If W is a subrepresentation of V , we would like to define an action of G on V/W by the natural choice of $g(v + W) = \varphi(g)(v) + W$. We must that this action is well defined. If we choose another $v' \in v + W$, then $v - v' \in W$ so that $\varphi(g)(v - v') \in W$ since W is G -invariant. Thus, the cosets $\varphi(g)(v) + W$ and $\varphi(g)(v') + W$ agree and this action is indeed well defined.

Definition 1.17. Let W be a G -subrepresentation of V . Then V/W forms a representation of G called the **quotient representation** of V under W , with the action $g(v + W) = \varphi(g)(v) + W$.

We recall also from linear algebra that given two vector spaces V_1 and V_2 , we can form the **direct sum** $V_1 \oplus V_2$ consisting of ordered pairs (v_1, v_2) where $v_1 \in V_1, v_2 \in V_2$.

Definition 1.18. Let V_1 and V_2 be representations of G . Then $V_1 \oplus V_2$ forms a representation of G called the **direct sum representation**, with the action $g(v_1, v_2) = (g \cdot v_1, g \cdot v_2)$.

1.5 Complete Reducibility and Unitarity

Definition 1.19. A representation is called **irreducible** if it contains no proper invariant subspaces. It is called **completely reducible** if it decomposes into a direct sum of irreducible subrepresentations.

Example 1.20. 1. Any irreducible representation is completely reducible.
2. Any 1-dimensional representations has no proper subspaces, and is thus irreducible.

Theorem 1.21. If A_1, A_2, \dots, A_r are linear operators on V and each A_i is diagonalizable, they are simultaneously diagonalizable if and only if they commute.

Proof. See [1, Theorem 5.1]. □

Theorem 1.22. Every complex representation of a finite abelian group is completely reducible, and every irreducible representation is 1-dimensional.

Proof. Take an arbitrary element $g \in G$. Since G is finite, we can find an integer n such that $g^n = 1$ and $\varphi(g)^n = Id$. Hence the minimal polynomial of $\varphi(g)$ divides $x^n - 1$. Recall that $x^n - 1$ has n distinct roots over \mathbb{C} , which are generated by taking powers of $\xi = e^{\frac{2\pi i}{n}}$. This means that the minimal polynomial $\varphi(g)$ factors into linear factors only over \mathbb{C} so that $\varphi(g)$ is diagonalizable. We conclude that each $\varphi(g)$ is (separately) diagonalizable since $g \in G$ was arbitrary.

Now, given any two elements $g_1, g_2 \in G$ we have

$$\begin{aligned} \varphi(g_1)\varphi(g_2) &= \varphi(g_1g_2) && \text{(since } \varphi \text{ is a homomorphism)} \\ &= \varphi(g_2g_1) && \text{(since } G \text{ is abelian)} \\ &= \varphi(g_2)\varphi(g_1) && \text{(since } \varphi \text{ is a homomorphism).} \end{aligned}$$

Thus the matrices $\{\varphi(g)\}$ commute, so we can apply 1.21 to conclude that $\{\varphi(g)\}$ are simultaneously diagonalizable. This basis $\{e_1, \dots, e_k\}$ yields the decomposition $V = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \dots \oplus \mathbb{C}e_n$. \square

We recall the following definition from linear algebra:

Definition 1.23. Let V be a complex vector space. A **Hermitian inner product** on V is a map $\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{C}$ that satisfies the following properties for all $u, v, w \in V$ and $c \in \mathbb{C}$:

1. $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$.
2. $\langle cu, v \rangle = c\langle u, v \rangle$.
3. $\langle u, v \rangle = \overline{\langle v, u \rangle}$.
4. $\langle v, v \rangle \geq 0$ with equality if and only if $v = 0$.

Definition 1.24. A representation φ of G on a complex vector space V is **unitary** if V has been equipped with a hermetian inner product $\langle \cdot, \cdot \rangle$ which is preserved by the action of G , that is,

$$\langle v, w \rangle = \langle \varphi(g)(v), \varphi(g)(w) \rangle \quad \forall v, w \in V, g \in G.$$

A representation is said to be **unitarisable** if it can be equipped with such a product (even without one being specified).

Theorem 1.25. [Weyl's unitary trick] *Finite-dimensional representations of finite groups are unitarisable.*

Proof. Take any Hermitian inner product on V , say $\langle \cdot, \cdot \rangle'$. We define a new inner product on V by *averaging over G* :

$$\langle v, w \rangle := \frac{1}{|G|} \sum_{g \in G} \langle \varphi(g)v, \varphi(g)w \rangle'.$$

This new inner product satisfies properties 1, 2, and 3 of Definition 1.23 by linearity. It remains to check positivity (4). Clearly $\langle v, v \rangle = 0$ when $v = 0$, since each term of the sum will equal zero. In the case where $v \neq 0$, observe that

$$\langle v, v \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \varphi(g)v, \varphi(g)v \rangle' \geq 0$$

since each term of the sum is non-negative by the positivity of $\langle \cdot, \cdot \rangle'$. The only problem would occur if each term of this sum is equal to zero. But $\langle \varphi(e)v, \varphi(e)v \rangle' = \langle v, v \rangle' > 0$. Thus $\langle v, v \rangle > 0$.

Finally, we show that our new inner product is G -invariant. For any $h \in G$, we have

$$\begin{aligned}
 \langle \varphi(h)v, \varphi(h)w \rangle &= \frac{1}{|G|} \sum_{g \in G} \langle \varphi(g)\varphi(h)v, \varphi(g)\varphi(h)w \rangle' \\
 &= \frac{1}{|G|} \sum_{g \in G} \langle \varphi(gh)v, \varphi(gh)w \rangle' && \text{(since } \varphi \text{ is a homomorphism)} \\
 &= \frac{1}{|G|} \sum_{k \in G} \langle \varphi(k)v, \varphi(k)w \rangle' && \text{(by a change of variables)} \\
 &= \langle v, w \rangle.
 \end{aligned}$$

□

Lemma 1.26. *Let V be a unitary representation of G and let $W \subseteq V$ be a G -invariant subspace. Then the orthogonal complement W^\perp is also G -invariant.*

Proof. Choose arbitrary elements $v \in W^\perp$ and $g \in G$. We need to show that $gv \in W^\perp$. Now for any $w \in W$, we have $\langle v, w \rangle = 0$. Thus $\langle gv, gw \rangle = g\bar{g}\langle v, w \rangle = 0$ for any $w \in W$. Notice that $w' = gw \in W$ since W is G -invariant. This implies that $\langle gv, w' \rangle = 0$, i.e. $gv \in W^\perp$. □

Theorem 1.27. *A finite-dimensional unitary representation of a group is fully reducible into unitary irreducible subrepresentations.*

Proof. Let V be a finite dimensional unitary representation of G . We proceed by induction on the dimension of V . If $\dim(V) = 1$, then V is necessarily irreducible. Now, suppose the theorem holds for all W with $\dim(V) \leq n - 1$ and suppose $\dim(V) = n$. If V is irreducible, we are done. Otherwise, there exists a proper G -invariant subspace $W (\neq 0, V)$. We can write $V = W \oplus W^\perp$ by Lemma 1.26. Applying the inductive hypothesis to W and W^\perp , we obtain a decomposition into irreducibles

$$V = (W_1 \oplus \dots \oplus W_j) \oplus (W_{j+1} \oplus \dots \oplus W_k).$$

□

Corollary 1.28. *Every complex representation of a finite group is completely reducible.*

Proof. Any such representation is unitarisable by Theorem 1.25. We can then apply Theorem 1.27 to obtain full reducibility. □

Bibliography

- [1] Keith Conrad. *The Minimal Polynomial and Some Applications*. <http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/minpolyandappns.pdf>. Online; accessed 12 December 2015. 2014.