REPRESENTATION THEORY OF FINITE GROUPS AND BURNSIDE'S THEOREM

ARIEH ZIMMERMAN

Abstract. In this paper we develop the basic theory of representations of finite groups, especially the theory of characters. With the help of the concept of algebraic integers, we provide a proof of Burnside's theorem, a remarkable application of representation theory to group theory.

Contents

1. Introduction 1
2. Characters 2
3. Some More Detailed Results 5
4. Integrality Properties of Characters 7
5. Burnside's Theorem 8
Acknowledgements 9
References 10

1. Introduction

Definition. A representation of a group G is a pair (V, ρ) where V is a complex vector space and $\rho : G \to \mathrm{GL}(V)$ is a group homomorphism.

When no confusion arises, we often refer to V or ρ as the representation itself. We will often denote $\rho(g)$ as ρ_g and $\rho(g)(v)$ as gv for $g \in G$ and $v \in V$. If V has finite dimension n, we call n the degree of the representation.

In this paper all representations are assumed to be finite dimensional.

Definition. Let (V, ρ) and (W, ρ') be representations of G. A homomorphism resp. isomorphism φ from the first to the latter is a linear transformation resp. isomorphism from V to W so that the diagram

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \rho_g \big\downarrow & & \big\downarrow \rho'_g \\ V & \xrightarrow{\varphi} & W \end{array}$$

commutes for every $g \in G$.

Definition. If (V, ρ) is a representation of G and V' is a subspace of V, and $\rho_g(V') \subseteq V'$ for all $g \in G$, we see that (V', ρ'), where $\rho' = \rho\,|_{V'}$, is also a representation of G. In this case we call V' a subrepresentation of V.

Date: August 17, 2015.

Definition. If a representation (V, ρ) contains a proper nonzero subrepresentation, we say that it is reducible. Otherwise, we say that it is irreducible.

Theorem 1. *If (V, ρ) is a representation of a finite group G and V' is a subrepresentation of V, then there is a complement W of V' that is also a subrepresentation of V.*

Proof. Let n be the degree of (V, ρ). Since V is a finite dimensional complex vector space, we can endow it with a hermitian inner product $(x \mid y) = \sum_{i=1}^{n} x_i \overline{y_i}$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ under a certain basis. Now, we can replace this inner product with a new inner product $\frac{1}{|G|} \sum_{g \in G} \langle \rho_g(x), \rho_g(y) \rangle$, which is clearly also hermitian. We show that the orthogonal complement W of V' under this inner product is stable under the action of G. That is, for $v' \in V'$, $w \in W$, and $h \in G$, we have

$$\frac{1}{|G|} \sum_{g \in G} \langle \rho_g(hw), \rho_g(v') \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho_{gh} w, \rho_{ghh^{-1}}(v') \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho_g w, \rho_g(h^{-1} v') \rangle = 0,$$

since the right action of h permutes G and $h^{-1} v' \in V' = W^{\perp}$. QED

Corollary. *Every representation of a finite group is isomorphic to a direct sum of irreducible representations.*

Proof. There is nothing to prove in the case that the representation has degree 1, since the only nonzero subspace of $\mathbb{C}$ is $\mathbb{C}$ itself. Let (V, ρ) be a representation of degree n. If V is irreducible we are finished. If not, let $V' \neq V$ be a nontrivial subrepresentation stable under the action of G. The above theorem shows that $W = (V')^{\perp}$ is also a subrepresentation of V. And V is isomorphic to $V' \oplus W$ as a representation of G. Since V' and W have dimension less than V, they are isomorphic to direct sums of irreducible subspaces via the induction hypothesis. QED

2. Characters

Definition. We define the character of a representation (V, ρ) to be the map $\chi_{(V,\rho)} : G \to \mathbb{C}$, where $\chi_{(V,\rho)}(g) = \mathrm{Tr}(\rho_g)$ for any $g \in G$.

When no confusion arises, we may write $\chi_{(V,\rho)}$ as χ.

Proposition 1. *If χ is a character of a representation of a finite group G of degree n, then for any $g, h \in G$,*

(i) $\chi(1) = n$
(ii) $\chi(g^{-1}) = \overline{\chi(g)}$
(iii) $\chi(gh) = \chi(hg)$.

Proof. *(i)* is true since the trace of the identity $n \times n$ matrix is n. Suppose $\lambda_1, \ldots, \lambda_m$ are eigenvalues of ρ_g with multiplicities $d_1, \ldots, d_m$. Then $1/\lambda_1, \ldots, 1/\lambda_m$ are eigenvalues of $\rho_{g^{-1}}$ with the same multiplicity. Note that ρ_g has finite order, so its eigenvalues are roots of unity. Thus $1/\lambda_i = \overline{\lambda_i}$ for $1 \leq i \leq m$, and *(ii)* follows. The final property of characters follows from the corresponding equation for the trace of matrices: $\mathrm{Tr}(\rho_g \rho_h) = \mathrm{Tr}(\rho_h \rho_g)$. QED

Definition. If (V_1, ρ^1) and (V_2, ρ^2) are representations of G, then we may define $V_1 \oplus V_2$ as a representation ρ by setting $\rho_g = \rho_g^1 \oplus \rho_g^2$ for any $g \in G$.

Proposition 2. *If (V_1, ρ^1) and (V_2, ρ^2) are representations of G and χ_1 and χ_2 are their characters respectively, then the character χ of $V_1 \oplus V_2$ has value $\chi_1 + \chi_2$.*

Proof. Let $g \in G$, and ρ_g^1 and ρ_g^2 have corresponding matrices R_g^1 and R_g^2. Then the matrix $R_g = \begin{pmatrix} R_g^1 & 0 \\ 0 & R_g^2 \end{pmatrix}$ representing $\rho_g^1 \oplus \rho_g^2$ clearly has trace $\mathrm{Tr}(R_g^1) + \mathrm{Tr}(R_g^2) = \chi_1(g) + \chi_2(g)$. QED

Schur's Lemma. *Let $f : V_1 \to V_2$ be a homomorphism between two irreducible representations (V_1, ρ_1) and (V_2, ρ_2) of G. Then*

1. *If the representations are not isomorphic, $f = 0$ and*
2. *if $(V_1, \rho_1) = (V_2, \rho_2)$, f is a homothety.*

Proof. We may assume $f \neq 0$, for if not the lemma would certainly hold. Then $\ker f \neq V_1$ and $\mathrm{Im}\, f \neq \{0\}$. In addition, if $w_1 \in \ker f$ and $w_2 \in \mathrm{Im}\, f$, we see $f \circ \rho_g^1(w) = \rho_g^2 \circ f(w) = \rho_g^2(0) = 0$ and $gf(w) = \rho_g^2 \circ f(w) = f \circ \rho_g^2(w) \in \mathrm{Im}(f)$, so that the kernel and image of f are invariant under the action of G. Because V_1 and V_2 are irreducible, we can deduce from this that $\ker f = \{0\}$ and $\mathrm{Im}\, f = V_2$, so f is an isomorphism, proving (1). For (2), since $\mathbb{C}$ is algebraically closed, f has some eigenvalue λ. If we let $f' = f - \lambda \cdot \mathrm{Id}$, then f' has a nonzero kernel, and one may easily check that f' is a homomorphism of representations. Thus, by the irreducibility of V_1, $f' = 0$, or $f = \lambda \cdot \mathrm{Id}$ is a homothety. QED

For complex valued functions $\phi, \psi : G \to \mathbb{C}$, where G is finite, we now denote $\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\psi(g^{-1})$ to be their *convolution*.

Theorem 2. *Let (V, ρ), (V', ρ') be two irreducible representations of a finite group G and χ, χ' be their characters respectively. If (V, ρ) and (V', ρ') are isomorphic, then $\langle \chi, \chi' \rangle = 1$. Otherwise, $\langle \chi, \chi' \rangle = 0$.*

Proof. Let f be an arbitrary linear map of V to V'. Then we can define f_0 as $\frac{1}{|G|} \sum_{g \in G} (\rho'_g)^{-1} f \rho_g$, which yields

$$(\rho'_h)^{-1} \circ f_0 \circ \rho_h = \frac{1}{|G|} \sum_{g \in G} (\rho'_h)^{-1} (\rho'_g)^{-1} f \rho_g \rho_h$$
$$= \frac{1}{|G|} \sum_{g \in G} (\rho'_{gh})^{-1} f \rho_{gh} = \frac{1}{|G|} \sum_{g \in G} (\rho'_g)^{-1} f \rho_g = f_0$$

for any $h \in G$, since multiplication by h permutes the elements of G. Hence f_0 is a homomorphism of representations. If ρ_g, ρ'_g and f are represented in matrix form as $(r_{ij}(g))$, $(r'_{i'j'}(g))$, and $(f_{i'i})$ respectively, we have

$$f_0 = \frac{1}{|G|} \sum_{g,j,j'} r'_{i'j'}(g^{-1}) f_{j'j} r_{ji}(g)$$

for every i, i'.

Assume that ρ is not isomorphic to ρ'. Then, by Schur's Lemma, we have $f_0 = 0$, and since f was chosen arbitrarily, we can consider the systems of values where $f_{j'j} = 1$ for any arbitrary choice of j and j', and is 0 otherwise, then equate coefficients to show that $\langle r'_{i'j'}, r_{ji}\rangle = 0$ for any i, i', j, j'. Thus, by the second property of Proposition 1,

$$\langle \chi, \chi' \rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi'(g^{-1}) = \frac{1}{|G|}\sum_{g,j,j'} r'_{j'j'}(g)r_{jj}(g^{-1}) = \sum_{j,j'}\langle r'_{j'j'}, r_{jj}\rangle = 0.$$

Assume, instead, that ρ and ρ' are isomorphic. Then Schur's Lemma now gives $f_0 = \lambda \cdot \mathrm{Id}$ for some scalar λ, so

$$n\cdot\lambda = \mathrm{Tr}(f_0) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(\rho_{g^{-1}} f \rho_g) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(f) = \mathrm{Tr}(f),$$

where n is the degree of the representation, and we get $\lambda = \frac{1}{n}\mathrm{Tr}(f)$. Since $f_0 = \lambda \cdot \mathrm{Id}$, we now have

$$\frac{1}{|G|}\sum_{g,j,j'} r'_{i'j'}(t^{-1}) f_{j'j} r_{ji}(t) = \lambda\delta_{i'i} = \frac{1}{n}\delta_{i'i}\sum_{j,j'}\delta_{j'j}f_{j'j},$$

which implies $\langle r'_{i'j'}, r_{ji}\rangle = \frac{1}{n}\delta_{i'i}\delta_{j'j}$. Therefore,

$$\langle \chi, \chi' \rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi(g^{-1}) = \frac{1}{|G|}\sum_{g,j,j'} r'_{j'j'}(g)r_{jj}(g^{-1})$$
$$= \sum_{j,j'}\langle r'_{j'j'}, r_{jj}\rangle = \frac{1}{n}\sum_{j,j'}\delta_{j'j}\cdot\delta_{j'j} = 1.$$

QED

Theorem 3. *Let V be a representation of a finite group G with character ϕ and $W_1 \oplus \ldots \oplus W_k$ a decomposition of V into irreducibles. Then, if W is any irreducible representation of G with character χ, the number of W_i isomorphic to W is $\langle \phi, \chi\rangle$.*

Proof. By Proposition 2, we have $\phi = \chi_1 + \cdots + \chi_k$, where χ_i is the character of W_i, which implies $\langle \phi, \chi\rangle = \langle \chi_1, \chi\rangle + \cdots + \langle \chi_k, \chi\rangle$. By Theorem 2 the i^{th} summand here is either 1 or 0 depending on whether or not W_i and W are isomorphic, and the result follows. QED

Corollary. *The number of W_i isomorphic to W in Theorem 3 does not depend on the choice of decomposition, and two representations with the same character are isomorphic.*

If a representation V decomposes into a direct sum of irreducible representations, and the irreducible representation V' occurs in this direct sum n times, from here forward we say V' occurs in V with multiplicity n.

Theorem 4. *If χ is the character of a representation V of a finite group G, then $\langle \chi, \chi\rangle = 1$ if and only if V is irreducible.*

Proof. The "if" part of the statement is given in Theorem 2. By Theorem 3 and its notation, we have $V \cong m_1W_1 \oplus \ldots \oplus m_kW_k$, where m_i is the integer $\langle \chi_i, \chi\rangle$. So $\langle \chi, \chi\rangle = m_1\langle \chi_1, \chi\rangle + \cdots + m_k\langle \chi_k, \chi\rangle = \sum_{i=1}^k m_i^2$, and the theorem is clear. QED

Definition. The regular representation of a finite group G is the pair (V, ρ) where $V = \mathbb{C}^{|G|}$ has a basis $\{e_g\}_{g\in G}$ and ρ is defined so that $\rho_h(e_g) = e_{hg}$ for any $h \in G$.

Proposition 3. *The character χ_G of the regular representation of a finite group G has $|G|$ as its value at 1 and 0 elsewhere.*

Proof. The first half of the statement follows from Proposition 1. To consider other values, note that action by elements of G permute elements of the basis, and nonidentity elements send no basis element to itself. Therefore, $\chi_G(h) = \mathrm{Tr}(\rho_h) = 0$ when $1 \neq h \in G$. QED

Corollary. *If V' is an irreducible representation of a finite group G, V' occurs in the regular representation of G with multiplicity equal to its degree n.*

Proof. Let χ' be the character of V'. By Propositions 1 and 3, we have

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi'(g^{-1}) = \frac{|G|}{|G|} \cdot \overline{\chi'}(1) = n,$$

and the proof follows from Theorem 3. QED

Definition. A class function on a group G is a function which is constant on conjugate classes; that is, $f(g) = f(hgh^{-1})$ for all $g, h \in G$.

Definition. For a finite group G, by $\hat{G}$ we denote the set of isomorphism classes of the irreducible representations of G.

Theorem 5. *The characters of all the elements of $\hat{G}$ form an orthonormal basis for the space H of class functions on G with respect to the Hermitian inner product $(\cdot \mid \cdot)$.*

Proof. Proposition 1 shows that these characters are an orthonormal system.

Assume f is a class function orthogonal to each of the characters of the irreducible representations. We prove $f = 0$. Let $\rho_f = \sum_{g \in G} f(g)\rho_{g^{-1}}$ for any irreducible representation ρ of G with degree n and character χ. Then, for any $h \in G$,

$$\rho_h^{-1}\rho_f\rho_h = \sum_{g \in G} f(g)\rho_h^{-1}\rho_{g^{-1}}\rho_h = \sum_{g \in G} f(h^{-1}gh)\rho_{h^{-1}g^{-1}h} = \rho_f,$$

since f is a class function and conjugation by h permute the members of G, preserving inverses. Therefore ρ_f satisfies the hypotheses of Schur's Lemma, and is hence a homothety $\lambda \in \mathbb{C}$. We calculate

$$n\lambda = \mathrm{Tr}(\lambda \cdot \mathrm{Id}) = \mathrm{Tr}(\rho_f) = \sum_{g \in G} f(g)\mathrm{Tr}(\rho_{g^{-1}}) = \sum_{g \in G} f(g)\chi(g^{-1}) = \langle f, \chi \rangle = 0,$$

so $\rho_f = \lambda = 0$. Since any representation can be decomposed into a direct sum of irreducible ones by the corollary to Theorem 1, combined with Proposition 2 this shows that $\rho_f = 0$ even for representations ρ that are not irreducible. If we take ρ to be the regular representation, then

$$0 = \rho_f e_1 = \sum_{g \in G} f(g)\rho_{g^{-1}}e_1 = \sum_{g \in G} f(g)e_{g^{-1}},$$

and by the linear independence of $\{e_g\}_{g \in G}$, we have $f = 0$ on G. QED

Corollary. *The number of elements of $\hat{G}$ is equal to the number of conjugacy classes of G.*

Proof. The dimension of the space H is clearly equal to the number of distinct conjugacy classes of G. By the above theorem, this is equal to the number of isomorphism classes of irreducible representations of G, which are completely determined by their characters. QED

3. Some More Detailed Results

Proposition 4. *Let G be a finite group. Let $h \in G$, $O(h)$ be the number of elements in the conjugacy class of h, j be an element of G not conjugate to h, and $\chi_1, \ldots, \chi_k$ the characters of the elements of $\hat{G}$. Then*

$$\sum_{i=1}^{k} \chi_i(h)\overline{\chi_i(h)} = \frac{|G|}{O(h)} \text{ and } \sum_{i=1}^{k} \chi_i(j)\overline{\chi_i(h)} = 0.$$

Proof. Let f_h be the class function whose value is one on the class of h and 0 elsewhere. Then, by Theorem 5,

$$f_h(g) = \sum_{i=1}^{k} \langle f_h, \chi_i \rangle \chi_i(g) = \sum_{i=1}^{k} \frac{O(h)}{|G|}\overline{\chi_i(h)}\chi_i(g) = \frac{O(h)}{|G|}\sum_{i=1}^{k} \chi_i(g)\overline{\chi_i(h)}$$

for $g \in G$. Since χ is a class function, the case where g is in the class of h gives the first statement, and the case where it is not gives the second. QED

Applying $h = 1$ to the proposition, we get the following corollary:

Corollary. *Let $\chi_1, \ldots, \chi_k$ be the characters of all elements of $\hat{G}$ and n_i be the degree of the representation associated with χ_i. Then $\sum n_i^2 = |G|$ and $\sum n_i \chi_i(g) = 0$ for any nonidentity element g of G.*

We now consider any representation of a finite group G a $\mathbb{C}[G]$-module by defining the action of $f \in \mathbb{C}[G]$ on $h \in G$ by $fh = \sum_G c_g gh$ when $f = \sum_G c_g g$ with $c_g \in \mathbb{C}$. In the case of the regular representation, one immediately finds that this is simply $\mathbb{C}[G]$ regarded as a module over itself.

It is clear that any representation of G is irreducible only if it, regarded as a $\mathbb{C}[G]$-module, is simple. Therefore, $\mathbb{C}[G]$ is semisimple - this is essentially a restatement of Theorem 1 - and any representation of G, by decomposition into irreducibles, is a direct sum of simple submodules by the corollary to Theorem 1.

Definition. Let G be a finite group, and $(W_1, \rho_1), \ldots, (W_k, \rho_k)$ representatives of all elements of $\hat{G}$. We define an algebra homomorphism $\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{End}(W_i)$ by linearly extending ρ_i. We then define a homomorphism $\tilde{\rho} : \mathbb{C}[G] \to \prod_{i=1}^{k} \mathrm{End}(W_i)$ by $\tilde{\rho}(f) = (\tilde{\rho}_1(f), \ldots, \tilde{\rho}_k(f))$.

Fourier Inversion Formula. *For $f \in \mathbb{C}[G]$, we put $f_i = \tilde{\rho}_i(f)$. Then, in the same notation as above,*

$$f = \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{k} n_i \mathrm{Tr}_{W_i}(\rho_i(g^{-1}) f_i) g,$$

where n_i is the degree of W_i.

Proof. Let χ_i be the character of W_i, and write f as $\sum_G c_g g$. Then the corollary to Proposition 4 gives

$$\frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{k} n_i\, Tr_{W_i}(\rho_i(g^{-1})f_i)g = \frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{k} n_i\, Tr_{W_i}\left(\rho_i(g^{-1})\sum_{g'\in G} c_{g'}\rho_i(g')\right)g$$

$$= \frac{1}{|G|}\sum_{g\in G}\sum_{g'\in G} c_{g'}\sum_{i=1}^{k} n_i\, Tr_{W_i}(\rho_i(g^{-1}g'))g = \frac{1}{|G|}\sum_{g\in G}\sum_{g'\in G} c_{g'}\sum_{i=1}^{k} n_i\chi_i(g^{-1}g')g$$

$$= \frac{1}{|G|}\sum_{g\in G}\sum_{g'\in G} c_{g'}\delta_{gg'}|G|g = \sum_{g\in G} c_g g = f$$

QED

Proposition 5. *$\tilde{\rho}$ as above is an algebra isomorphism.*

Proof. Let $F : \prod \mathrm{End}(W_i) \to \mathbb{C}[G]$ denote the Fourier inversion formula. The previous proof shows that $F \circ \tilde{\rho} = 1 \mid_{\mathbb{C}[G]}$, implying injectivity. Now, to show bijectivity, we need only compare dimensions. Using the corollary to Proposition 4,

$$\dim(\mathbb{C}[G]) = |G| = \sum_{i=1}^{k} n_i^2 = \dim\left(\prod_{i=1}^{k}\mathrm{End}(W_i)\right).$$

QED

Proposition 6. *$\tilde{\rho}$ as above maps the center of $\mathbb{C}[G]$ isomorphically onto $\mathbb{C}^k$, where k is the number of conjugacy classes of G.*

Proof. The center of $\mathbb{C}[G]$ consists precisely of those elements commuting with each $g \in G$. Applying $\tilde{\rho}$, by the corollary to Theorem 5, the image of this center then consists of all members of $\prod \mathrm{End}(W_i)$ commuting with each $(\rho_1(g), \ldots, \rho_k(g))$. Each entry of such functions is a homomorphism of representations, or, by Schur's Lemma, a homothety. Conversely, every k-tuple of homotheties clearly satisfies this commutativity. Pairing these homotheties with their ratios in $\mathbb{C}$, the isomorphism is shown. QED

4. Integrality Properties of Characters

Lemma. *A complex number c is integral over $\mathbb{Z}$ i.e., c is the root of a monic polynomial over $\mathbb{Z}$, if and only if the subring $\mathbb{Z}[c]$ of $\mathbb{C}$ is finitely generated as an abelian group.*

Proof. Assume c is integral over $\mathbb{Z}$. Then there is some monic $f \in \mathbb{Z}[X]$ with $f(c) = 0$, or

$$c^n + a_1 c^{n-1} + \cdots + a_1 = 0$$

for some $a_1, \ldots, a_n \in \mathbb{Z}$. This shows that any power of c greater than n can be reduced to a $\mathbb{Z}$-linear combination of $c^{n-1}, \ldots, 1$, making $\mathbb{Z}[c]$ a finitely generated abelian group. Assume conversely that $\mathbb{Z}[c]$ is finitely generated, and let $a_1, \ldots, a_m$ be its generators. Then there are $f_i \in \mathbb{Z}[X]$ such that $a_i = f_i(c)$ for $1 \le i \le m$. Now let $N = \max\{\deg f_1, \ldots, \deg f_m\} + 1$. Then there are $b_i \in \mathbb{C}$ with $c^N = \sum b_i a_i = \sum b_i f_i(c)$. Therefore c is a root of the monic polynomial $X^n - \sum b_i f_i(X)$, which has integral coefficients, making c an algebraic integer. QED

Theorem 6. *Every element in the image of any character χ of any representation ρ of a finite group G is an algebraic integer.*

Proof. For $h \in G$, since G is finite, we see that ρ_h has a finite order m. Therefore, if λ is an eigenvalue of ρ_h, we have λ^m an eigenvalue of $\rho_h^m = \rho_1$. Since 1 is the only eigenvalue of ρ_1, this means $\lambda^m = 1$. Therefore $\chi(h)$, which is the sum of eigenvalues of ρ_h with their algebraic multiplicities, is a sum of m^{th} roots of unity. Hence $\chi(h)$ is contained in $\mathbb{Z}[e^{2\pi i/m}]$, which is a finitely generated abelian group. By the above lemma, we see that $\chi(h)$ is an algebraic integer. QED

Proposition 7. *Let $f = \sum_G c_g g$ be in the center of $\mathbb{C}[G]$, with G a finite group, and assume the c_g are algebraic integers. If ρ is an irreducible representation of G with character χ, then $\frac{1}{n}\sum_G c_g\chi(g)$ is an algebraic integer.*

Proof. We first show that f is integral over $\mathbb{Z}$.

For any $h \in G$, we have $\sum_G c_g h^{-1}gh = h^{-1}fh = f = \sum_G c_g g$. This shows that the coefficients of every conjugate of each g is c_g. We may therefore rewrite f as $\sum_{i=1}^k c_i s_i$, where s_i is the sum of the members of the i^{th} conjugacy class of G. Since c_i is an algebraic integer for each i, to prove that f is integral over $\mathbb{Z}$, it suffices to prove that each s_i is integral over $\mathbb{Z}$. This follows from the lemma preceding Theorem 6 and the observation that $\mathbb{Z}s_1 \oplus \ldots \oplus \mathbb{Z}s_k$ is a subring with identity of the center of $\mathbb{C}[G]$.

Now, one easily checks that $\rho_h^{-1} f \rho_h = f$ as a result of the coefficients of conjugate elements of G being equal, showing that f is a homomorphism of representations. Hence, by Schur's Lemma, it is a homothety $\lambda \cdot \mathrm{Id}$, and comparing traces gives

$$n\lambda = \mathrm{Tr}(\lambda \cdot \mathrm{Id}) = \mathrm{Tr}(f) = \sum_{g\in G} c_g \mathrm{Tr}(\rho_g) = \sum_{g\in G} c_g \chi(g),$$

or $\lambda = \frac{1}{n}\sum_G c_g\chi(g^{-1})$. Since $\lambda \cdot \mathrm{Id} = f$ is integral over $\mathbb{Z}$, λ is an algebraic integer, proving the statement. QED

Corollary. *If ρ is an irreducible representation of a finite group G of degree n, then $n \mid |G|$.*

Proof. Let ρ have character χ. We see that the function $f = \sum_G \chi(g^{-1})g$ is in the center of $\mathbb{C}[G]$, since χ is a class function. We may therefore apply the proposition above, showing

$$\lambda = \frac{1}{n}\sum_{g\in G}\chi(g^{-1})\chi(g) = \frac{|G|}{n}\langle\chi,\chi\rangle = \frac{|G|}{n}$$

is an algebraic integer. The statement then follows since the only rational algebraic integers are members of $\mathbb{Z}$. QED

5. Burnside's Theorem

Lemma 1. *If G is a group of order p^a, with p prime, then G is solvable.*

Proof. We induct on a. The case of $a = 0$ is trivial. Assume the statement holds for all integers up to $a - 1$. We show it holds when $|G|= p^a$. Assume that G has trivial center. Since the order of any conjugacy class of G divides the order of G, we see that each conjugacy class other than $\{1\}$ has order p^{k_i} for some $k_i \in \mathbb{N}$, with i indexing the conjugacy classes. Hence, by the class equation,

$$|G| = |Z(G)| + \sum_i p^{k_i} = 1 + \sum_i p^{k_i},$$

where $Z(G)$ is the center of G. This is a contradiction since $p \mid |G|$. Therefore $Z(G)$ must be a nontrivial normal subgroup, and because $Z(G)$ and $G/Z(G)$ are both solvable by the induction hypothesis, G is solvable. QED

Lemma 2. *Let h be a nonidentity element of a finite group G. Let $O(h)$ be the number of elements in the conjugacy class of h, and suppose $O(h) = p^a$ for some prime number p. Then there is some irreducible representation ρ of G with kernel $N \neq G$ such that $\rho(h)$ is in the center of* $\mathrm{Im}(\rho)$.

Proof. We first find a character χ of a nontrivial irreducible representation of G such that $\chi(h) \neq 0$ and $p \nmid \chi(1)$. Suppose such character does not exist. With the same notation as Proposition 4, we have

$$1 + \sum_{\chi_i \neq 1} \chi_i(1)\chi_i(h) = \sum_{i=1}^{k} \chi_i(1)\overline{\chi_i(h^{-1})} = 0.$$

By our assumption p divides each $\chi_i(1)$, so, subtracting 1 and dividing each side by p, we find that $-\frac{1}{p}$ is a $\mathbb{Z}$-linear combination of the $\chi_i(h)$. Theorem 6 would then imply that $-\frac{1}{p}$ is an algebraic integer, a contradiction.

Let ρ be the representation associated with the character χ found above, and let $N = \ker \rho$. We know that $N \neq G$ since ρ is not trivial.

Define $v : G \to \mathbb{C}$ so that $v(g) = 1$ if g is in the conjugacy class of h and $v(g) = 0$ otherwise. Then v is a class function, so, by Proposition 7,

$$\frac{1}{\chi(1)} \sum_{g \in G} v(g^{-1})\chi(g^{-1}) = \frac{O(h)}{\chi(1)}\chi(h)$$

is an algebraic integer, and therefore has norm $\frac{O(h)}{\chi(1)}|\chi(h)|$ that is an integer. Since $p \nmid \chi(1)$, this shows $\chi(1) \mid |\chi(h)|$. Note that $\chi(h) \neq 0$ and $\chi(h)$ is a sum of $\chi(1)$ roots of unity. By the triangle inequality, we deduce that ρ_h has only one eigenvalue. Note that ρ_h is diagonalizable since it has finite order. Therefore, ρ_h is a scalar matrix, and is in the center of $\mathrm{Im}(\rho)$. QED

Burnside's Theorem. *Every group of order $p^a q^b$, with p and q prime, is solvable.*

Proof. We induct on the pair (a, b). The base cases where $a = 0$ or $b = 0$ follow from Lemma 1.

If G has nontrivial center Z, then G/Z and Z are solvable by the induction hypothesis, so G is solvable.

Assume instead that G has trivial center. Then there is some nonidentity $h \in G$ such that $q \nmid O(h)$. This is because, if no such h exists, since the sum of the orders of the conjugacy classes of G is $|G|$, we would have $p^a q^b$ equal to a multiple of q plus 1, a clear contradiction. So we may apply Lemma 2 to find a representation ρ of G with kernel $N \neq G$ and $\rho(h)$ in the center of $\mathrm{Im}(\rho)$. If N were trivial, then $G \cong \mathrm{Im}(\rho)$, putting h at the center of G, a contradiction. Hence both N and G/N have order less than $|G|$ and are solvable by the induction hypothesis, implying G is solvable. QED

Acknowledgements

I am deeply indebted to my mentors, Zhiyuan Ding and Yun Cheng, for their patience and enthusiasm in guiding me to a thorough understanding of this interesting topic. This paper would not have developed if not for Zhiyuan's invaluable experience and advice in editing my writing to develop clarity, and Yun's insightful comments and help in choosing a topic. I also thank REU director Peter May for his hard work every year to help encourage undergraduates looking to explore their passions in pure mathematics. Lastly, I'd like to express my appreciation for Robert Fefferman and the administration of the University of Chicago math department.

References

[1] Dummit, David S.; Foote, Richard M. (2004), Abstract algebra, Third Edition, John Wiley & Sons Inc., Hoboken, NJ.

[2] Fulton, William; Harris, Joe (1991), Representation theory. A first course, Graduate Texts in Mathematics, Readings in Mathematics 129, New York: Springer-Verlag, ISBN 978-0-387-97495-8, MR 1153249, ISBN 978-0-387-97527-6

[3] Serre, Jean-Pierre (1977). Linear Representations of Finite Groups. Springer-Verlag. ISBN 0-387-90190-6.