REPRESENTATION THEORY

KATHERINE TAYLOR

Abstract. Representation theory is about carrying structures in abstract algebra to structures in linear algebra. In this paper we cover the basics of representations of finite groups, paying special attention to abelian groups. We also include some basic character theory and a proof of Burnside's Theorem.

1. Introduction: Matrix Groups

The set of $n \times n$ invertible matrices forms a group under multiplication, since matrix multiplication is associative and there's an identity matrix and inverses. We can also talk about adding and subtracting matrices elementwise, but the multiplicative group is more interesting and useful for our purposes. It'd be interesting to just talk about matrices by themselves, but there's another way of looking at it. An $n \times n$ invertible matrix M will, when multiplied on the right by any vector v in an n-dimensional vector space V, output another n-dimensional vector $u \in V$.

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}$$

Definition 1.1 (Linear Transformation)**.** *Let U and V be vector spaces over a field F. Then a function $T : U \to V$ is a linear transformation if it satisfies $T(u_1 + u_2) = T(u_1) + T(u_2)$ and $T(cu_1) = cT(u_1)$ for all $u_1, u_2 \in U$ and all $c \in F$.*

A linear transformation is invertible if it has an inverse. Invertible linear transformations from a vector space V to itself form a group, since function composition is associative and there's an identity element T defined by $T(v) = v$. It's fairly easy to check that the operation of multiplication by M is a linear transformation from V to itself. In fact, in a finite vector space V, every linear transformation from V to itself can be written in matrix form. (But note that which matrix corresponds to which linear transformation depends on the choice of basis.) So, if V is n-dimensional over a field F, then the group under multiplication of $n \times n$ invertible matrices with entries in F corresponds to the group we call $GL(V)$, the group of invertible linear transformations on V. Now that we've developed this interpretation of matrix groups, we can say what a representation is.

Definition 1.2 (Representation)**.** *A representation of a group G is a group action of G on the vector space V through linear transformations, or equivalently, a homomorphism $\phi : G \to GL(V)$. We denote a representation of G by (V, ϕ).*

Once we pick a basis, a representation is a homomorphism from a finite group to a group of matrices. Representations can be defined for other things, like Lie algebras, but we'll stick to finite groups. Since everything is easier in an algebraically closed field, we'll also stick to vector spaces of the form $V = \mathbb{C}^n$, though there are representations for more exotic vector spaces. What makes representations really cool, even before we've seen any of the theory, is that they give a concrete, visible structure to groups. Linear algebra concepts like vector subspaces, eigenvectors/eigenvalues,

Date: June 7, 2020.

inner products, similar matrices, and trace, interact in interesting ways with concepts from group theory. They can also tell us new things about groups that would be hard to figure out using only group theory.

Let (V, ϕ) be a representation. When ϕ is "faithful", or injective, G is isomorphic to a subgroup of $GL(V)$. In other words, groups with injective representations can be written as groups of matrices. Here's an example of an injective representation for S_3. (We'll say the vector space is $\mathbb{C}^3$ with the usual basis, so $\phi : S_3 \to GL(\mathbb{C}^3)$.)

$$\phi(e) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \phi((12)) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \phi((13)) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$\phi((23)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \phi((123)) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \phi((132)) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Notice that each matrix will simply permute the entries of a vector, so this corresponds to the group action of S_3 on a set of 3 elements. There's nothing special about using S_3 here. In general, there is an n-dimensional injective representation for S_n, for which each element s of S_n is sent to a matrix $\phi(s)$ that performs the permutation s on the basis vectors of the vector space. So, every symmetric group is isomorphic to a group of matrices. And every finite group is isomorphic to a subgroup of a symmetric group (Cayley's Theorem), so we can create an injective homomorphism from any finite group to some group of matrices. We reach the following conclusion:

Proposition 1.3. *Every finite group is isomorphic to a group of matrices.*

2. Basic Concepts

Now that we've written all our finite groups as matrix groups, we can start applying linear algebra techniques to them. We define the following terms:

Definition 2.1 (Invariant subspace)**.** *A vector subspace $V' \subseteq V$ is called invariant if (V, ϕ) is a representation and $\phi(g)v' \in V'$ for all $g \in G$, $v' \in V'$.*

Definition 2.2 (Subrepresentation)**.** *If (V, ϕ) is a representation and $V' \subseteq V$ is invariant, we call (V', ϕ) a subrepresentation of (V, ϕ).*

A subrepresentation is itself a representation. Also, every representation (V, ϕ) has two trivial subrepresentations, which are $(\{0\}, \phi)$ and (V, ϕ). The vector subspace $U = \{[z, z, z] : z \in \mathbb{C}\}$ of $\mathbb{C}^3$ is invariant under the representation of S_3 we defined earlier, since $[z, z, z]$ is still $[z, z, z]$ after any permutation. The vector subspace $W = \{[x, y, z] : x + y + z = 0\}$ is also invariant under our representation of S_3 since permuting the entries of a vector won't change the fact that the entries sum to zero. (U, ϕ) and (W, ϕ) are both subrepresentations of (V, ϕ), and they're both representations of S_3.

Definition 2.3 (Reducibility)**.** *We call (V, ϕ) irreducible if it has no subrepresentations other than $(\{0\}, \phi)$ and itself, and reducible otherwise.*

A one-dimensional representation, like $\{[z, z, z] : z \in \mathbb{C}\}$, is automatically irreducible, because a one-dimensional vector space has no subspaces to use for subrepresentations other than $\{0\}$ and itself. For representations of greater dimension, it can be much harder to determine irreducibility. Irreducible representations are the "building blocks" of representation theory, sort of like simple groups in group theory.

Definition 2.4 (Full reducibility)**.** *(V, ϕ) is called fully reducible if V is a direct sum of irreducible invariant subspaces.*

That is, V is fully reducible if $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$ where each W_i forms an irreducible subrepresentation of (V, ϕ) under ϕ. If V is fully reducible, then there is a very nice-looking matrix group for the set of linear transformations given by $\{\phi(g) : g \in G\}$. We start by finding bases for each of the W_i's. Then, since V is a direct sum of the W_i's, we can combine all these bases to get a basis for V. In this basis, the matrix group generated by ϕ consists of block-diagonal matrices: all zeroes except for k square blocks on the diagonal, with each block corresponding to one of the W_i's.

The following is another example of a representation and a more rigorous proof of Proposition 1.3. Given a finite group G, define its *regular representation* as follows: Let V be a complex vector space with dimension $n = |G|$. Define a basis $\{e_g : g \in G\}$, so that each element g has a corresponding basis vector. Let ϕ be defined by

$$\phi(g)e_h = e_{gh}$$

for every g in G. (We extend ϕ to any $v \in V$ by writing v as a linear combination of basis vectors.) We have $\phi(g_1)\phi(g_2)e_h = \phi(g_1)e_{g_2h} = e_{g_1g_2h} = \phi(g_1g_2)e_h$, so ϕ is a homomorphism. Also, $\ker(\phi) = \{g \in G : e_{gh} = e_h\} = e$, so ϕ is injective. This makes (V, ϕ) a representation of G. For each $g \in G$, $\phi(g)$ is a permutation on the basis vectors, which can be written as a permutation matrix for that basis. So, every finite group G is isomorphic to a group of matrices.

3. Finite Abelian Groups

Suppose G is a finite group of order n with a complex representation (V, ϕ). If $g \in G$, what can we say about the matrix $\phi(g)$? We know that for each $g \in G$, $g^n = e$. That implies $\phi(g^n) = \phi(g)^n = \phi(e) = I$, the identity matrix. So, $\phi(g)^n - I = 0$, which implies that the minimal polynomial of $\phi(g)$ divides $x^n - 1 = 0$. Thus the minimal polynomial of $\phi(g)$ has no repeated roots and only linear factors, so $\phi(g)$ is diagonalizable. Further, its eigenvalues are nth roots of unity. We conclude:

Proposition 3.1. *If (V, ϕ) is a representation of a finite group G, then for every $g \in G$, $\phi(g)$ is diagonalizable and its eigenvalues are roots of unity.*

However, note that there's not necessarily a basis for which all $\phi(g)$ are simultaneously diagonalizable. Next assume G is abelian, so $\phi(g_1)\phi(g_2) = \phi(g_2)\phi(g_1)$ for all $g_1, g_2 \in G$. It is a fact of linear algebra that any group of separately diagonalizable, commuting matrices must be simultaneously diagonalizable, so if G is abelian there must be some basis for which every $\phi(g)$ is diagonal. To sum up:

Theorem 3.2. *if G is a finite abelian group of order n then any complex representation of G consists of a group of simultaneously diagonalizable matrices whose eigenvalues are nth roots of unity.*

In a group of diagonal matrices, each of the basis elements is invariant and forms a one-dimensional subrepresentation, so any complex representation of an abelian group G is fully reducible. Furthermore, any irreducible representation of G is just a homomorphism from G to a group with elements in the nth roots of unity. If the group G is cyclic and generated by the element g, then a complex representation (V, ϕ) is entirely determined by what $\phi(g)$ is. Letting $e^{2\pi i/5} = \zeta$, here's an example of a representation for $\mathbb{Z}/5\mathbb{Z}$ on $\mathbb{C}^4$:

$$\phi(0) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \phi(1) = \begin{bmatrix} \zeta & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & \zeta^2 \end{bmatrix}$$

$$\phi(2) = \begin{bmatrix} \zeta^2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 \\ 0 & 0 & 0 & \zeta^4 \end{bmatrix} \quad \phi(3) = \begin{bmatrix} \zeta^3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \zeta^3 & 0 \\ 0 & 0 & 0 & \zeta^1 \end{bmatrix}$$

$$\phi(4) = \begin{bmatrix} \zeta^4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^3 \end{bmatrix}$$

The choice of which roots of unity go on the diagonal was sort of arbitrary – this is far from the only representation of $\mathbb{Z}/5\mathbb{Z}$ on $\mathbb{C}^4$. This raises the question of how many representations of $\mathbb{Z}/5\mathbb{Z}$ there are, exactly. Since any complex representation of $\mathbb{Z}/5\mathbb{Z}$ is determined by which collection of 5th roots of unity lie on the diagonal of $\phi(1)$, it seems like counting representations is the same as counting how many combinations of 5th roots of unity we can make. This is correct, but to formalize this argument and get some insight into nonabelian groups, we need some more theory.

4. Unitarity and Reducibility

Recall that an inner product space is a vector space equipped with an inner product. An inner product is like a generalization of the dot product, taking in two vectors and outputting a scalar. In a complex vector space the usual inner product is the Euclidean inner product:

$$\langle u, v \rangle = u_1\bar{v}_1 + u_2\bar{v}_2 + \cdots + u_n\bar{v}_n$$

Inner products have a longer definition which we will not go into here. Once we have an inner product, we can define the norm $||v||$, which is like a generalization of "length":

$$||v|| = \sqrt{\langle v, v \rangle}$$

Definition 4.1 (Isometry)**.** *A matrix over an inner-product space is called an isometry if*

$$\langle Mu, Mv \rangle = \langle u, v \rangle$$

for all $u, v \in V$.

(An isometry over $\mathbb{C}^n$ with the Euclidean inner product is called a unitary matrix, and has the property that its conjugate transpose is also its inverse.) Isometries have lots of nice properties. A matrix M is an isometry if and only if it preserves norms, meaning $||Mv|| = ||v||$ for all $v \in V$. So, we can think of isometries as "length-preserving" functions. The determinant of an isometry always has magnitude 1. Another equivalent condition: M is an isometry if and only if V has an orthonormal basis for which M is diagonal with eigenvalues of magnitude 1. (An orthonormal basis is a basis $\{e_1, \ldots e_n\}$ such that for all $i \neq j$, $\langle e_i, e_j \rangle = 0$ and for all i, $||e_i|| = 1$.)

We can apply this new vocabulary to our results for finite abelian groups. Assuming an orthonormal basis, we reach the conclusion that any finite abelian group has a representation where every matrix is an isometry. It turns out this result can be generalized.

Definition 4.2 (Unitary representation)**.** *A representation (V, ϕ) of G is called unitary if there exists an inner product $\langle \cdot, \cdot \rangle$ on V such that for all $g \in G$, $\phi(g)$ is an isometry.*

Theorem 4.3 (Weyl's Unitary Trick)**.** *Every representation of a finite group can be made unitary.*

Proof. Start with a finite group G and a representation (V, ϕ) with an inner product $\langle \cdot, \cdot \rangle$ on V. To construct a unitary representation, we'll invent a new inner product $\langle\langle \cdot, \cdot \rangle\rangle$ that is preserved by $\phi(g)$ for all $g \in G$. We claim that the following definition works:

$$\langle\langle u, v \rangle\rangle = \frac{1}{|G|} \sum_{g \in G} \langle \phi(g)u, \phi(g)v \rangle$$

We can check that this satisfies the definition of an inner product. The remaining property we want is that if for $h \in G$ we take $\langle\langle \phi(h)u, \phi(h)v\rangle\rangle$ instead of $\langle\langle u, v\rangle\rangle$, we'll get the same sum overall. We have

$$\begin{aligned}\langle\langle \phi(h)u, \phi(h)v\rangle\rangle &= \frac{1}{|G|}\sum_{g\in G}\langle \phi(g)\phi(h)u, \phi(g)\phi(h)v\rangle \\ &= \frac{1}{|G|}\sum_{g\in G}\langle \phi(gh)u, \phi(gh)v\rangle\end{aligned}$$

If g ranges over all elements of G and h is fixed, gh will also range over all elements of G. So, we are summing over the same set and

$$\langle\langle \phi(h)u, \phi(h)v\rangle\rangle = \langle\langle u, v\rangle\rangle$$

for all $h \in G$. Therefore, there exists an inner product such that for all $g \in G$, $\phi(g)$ is an isometry, implying that (V, ϕ) is unitary. □

Earlier we made the claim that irreducible representations are like the "building blocks" of representation theory. Maschke's Theorem justifies that claim.

Theorem 4.4 (Maschke's Theorem)**.** *Any complex representation of a finite group is fully reducible.*

Proof. We will proceed by induction. We know that that any one-dimensional representation is irreducible and therefore fully reducible. So, suppose that any complex representation of a finite group with dimension less than n is fully reducible. Next, suppose (V, ϕ) is a complex representation of some finite group G, and suppose $\dim V = n$. Because of our last result, there is some inner product $\langle\cdot,\cdot\rangle$ preserved by $\phi(g)$ for each $g \in G$. Either V is irreducible, in which case it is fully reducible, or it has some invariant subspace U. Consider the orthogonal complement of U, denoted $U^\perp$. (Recall that the orthogonal complement of a subspace $U \subseteq V$ is $U^\perp = \{v \in V : \langle u, v\rangle = 0, \forall u \in U\}$.) Now consider some $u \in U$, some $v \in U^\perp$, and some $g \in G$. Since U is invariant, $\phi(g^{-1})u = u' \in U$, so $u = \phi(g)u'$. Then, since $\langle\cdot,\cdot\rangle$ is preserved by $\phi(g)$, we have

$$\langle u, \phi(g)v\rangle = \langle \phi(g)u', \phi(g)v\rangle = \langle u', v\rangle$$

By the definition of $U^\perp$, $\langle u', v\rangle = 0$, so $\langle u, \phi(g)v\rangle = 0$. So, for any v in $U^\perp$ and any $g \in G$, $\phi(g)v$ is also in $U^\perp$, which means $U^\perp$ is an invariant subspace. Thus (U, ϕ) and $(U^\perp, \phi)$ are subrepresentations of (V, ϕ), and since they're orthogonal complements, we have $V = U \oplus U^\perp$. By the inductive hypothesis, since U and $U^\perp$ both have dimension less than V they can be written as direct sums of irreducible subspaces $U_1 \oplus U_2 \oplus \cdots \oplus U_k$ and $W_1 \oplus W_2 \oplus \cdots \oplus W_m$, respectively. So $V = U_1 \oplus \cdots \oplus U_k \oplus W_1 \oplus \cdots \oplus W_m$ and (V, ϕ) is fully reducible. □

5. Non-Basic Concepts (Plus More Abelian Groups)

In a minute we will return to counting how many representations of $\mathbb{Z}/5\mathbb{Z}$ there are, but first we need some way to formalize whether two representations are "the same" or "different".

Definition 5.1 (Intertwining operator)**.** *If (V, ϕ) and (V', ϕ') are representations of G, then a linear transformation $L : V \to V'$ is an intertwining operator if $\phi'(g)L = L\phi(g)$ for all $g \in G$.*

Such a function L preserves both the linear structure of V and the group structure of G.

Definition 5.2 (Isomorphism)**.** *If an intertwining operator $L : V \to V'$ is invertible, then L is called an isomorphism and (V, ϕ) and (V', ϕ') are called isomorphic.*

This is what makes intertwining operators useful for us. Invertibility allows us to write $\phi'(g) = L\phi(g)L^{-1}$, meaning that (V, ϕ) and (V', ϕ') are isomorphic if and only if $\phi(g)$ and $\phi'(g)$ are similar (conjugate) matrices by some matrix L for all $g \in G$. Isomorphism is an equivalence relation. It means representations are "essentially the same" in the same way as group isomorphism means

groups are "essentially the same". This means we can split up the representations of G into isomorphism classes.

As an example, suppose (V, ϕ) and (V', ϕ') are representations of $\mathbb{Z}/5\mathbb{Z}$ over $\mathbb{C}^4$ such that $\phi(1)$ and $\phi'(1)$ have the same roots of unity on the diagonal, but in a different order:

$$\phi(1) = \begin{bmatrix} \zeta & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & \zeta^2 \end{bmatrix} \quad \phi'(1) = \begin{bmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

There is some permutation matrix P which permutes the roots of unity from their positions in $\phi(1)$ to their positions in $\phi'(1)$. Then $\phi'(1)$ would perform the same transformation as $P\phi(1)P^{-1}$, so $\phi'(1) = P\phi(1)P^{-1}$. That implies $\phi'(g) = P\phi(g)P^{-1}$ for all $g \in \mathbb{Z}/5\mathbb{Z}$, so $\phi(g)$ and $\phi'(g)$ are all conjugate by P. In this case we can compute P as performing the permutation (243) on the basis vectors, so

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

and in matrix form the isomorphism $\phi'(1) = P\phi(1)P^{-1}$ is

$$\begin{bmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \zeta & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & \zeta^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

In general, L does not have to be a permutation matrix. Conjugation by any invertible matrix L produces a representation of G which is isomorphic to (V, ϕ).

Let's return to our earlier example of $\mathbb{Z}/5\mathbb{Z}$. Possible representations of $\mathbb{Z}/5\mathbb{Z}$ consist of diagonal matrices with roots of unity on the diagonal, which are similar if and only if they have the same entries on the diagonal (but possibly in a different order). A representation of $\mathbb{Z}/5\mathbb{Z}$, or any cyclic group, is determined by the matrix of the generating element. So, the set of isomorphism classes of k-dimensional representations of a cyclic group of order n is the set of all possible sets of entries on the diagonal of the generating element, which is just the set of all (unordered) k-tuples of nth roots of unity.

Schur's Lemma gives us some more insight into intertwining operators and isomorphisms between irreducible representations.

Theorem 5.3 (Schur's Lemma)**.** *If (V, ϕ) and (W, ϕ') are irreducible representations of G, then an intertwining operator L from V to W is either 0 or an isomorphism. If (V, ϕ) is an irreducible complex representation of a finite group G, then every intertwining operator $L : V \to V$ is a scalar.*

Proof. Suppose there is a nontrivial intertwining operator L from V to W. What is the null space of L? First recall that the null space of a linear transformation is a vector subspace. Next, if $v \in V$ is such that $Lv = 0$, then $L\phi(g)v = \phi'(g)Lv = \phi'(g)0 = 0$ for all $g \in G$. Thus the null space of L forms an invariant subspace of V. Since V is irreducible, the null space of L must be the zero vector, and L is injective. Now consider the image of L, which forms a vector subspace of W. If $w \in W$ is such that $w = Lv$ for some $v \in V$, then $\phi'(g)w = \phi'(g)Lv = L\phi(g)v$, so the image of L is an invariant subspace of W. W is irreducible, so the image of L must be W, making L surjective and thus bijective. We have proved that an intertwining operator between irreducible representations must either be trivial or an isomorphism.

Now for the proof of the second part. Suppose L is an intertwining operator from V to itself. Then for all $g \in G$, $\phi(g)L = L\phi(g)$. Since L is an invertible linear function over $\mathbb{C}$, it has some

eigenvalue $\lambda \in \mathbb{C}$. Let $v \in V$ be an eigenvector for λ. We have

$$L\phi(g)v = \phi(g)Lv = \phi(g)\lambda v = \lambda\phi(g)v$$

But if $L\phi(g)v = \lambda\phi(g)v$, then $\phi(g)v$ must also be an eigenvector of L with eigenvalue λ. So, $\phi(g)v$ is an eigenvector with eigenvalue λ for every $g \in G$. The set $\{\phi(g)v : g \in G\}$ must span V (otherwise it would form an invariant subspace, and we know V is irreducible). Therefore, every vector in V is an eigenvector of L with eigenvalue λ, so L is just the matrix λI. □

The part about $L : V \to V$ being a scalar is only true for complex vector spaces (it's sometimes called "Schur's Lemma over $\mathbb{C}$").

6. Characters

Definition 6.1 (Character of a representation)**.** *Let (V, ϕ) be a complex representation of a finite group G. The character of (V, ϕ) is the function $\chi_V : G \to \mathbb{C}$ which sends g to the trace of the matrix $\phi(g)$.*

The character function produces a more condensed form of a representation. We see that

$$\chi_V(e) = \mathrm{Tr}(\phi(e)) = \mathrm{Tr}(I) = \dim V.$$

From Proposition 3.1, we may assume that $\phi(g)$ is a diagonal matrix with roots of unity on the diagonal. If ζ is a root of unity, then $\overline{\zeta} = \frac{1}{\zeta}$, so the trace of $\phi(g^{-1})$ is the complex conjugate of the trace of $\phi(g)$. This gives us another character identity:

$$\chi_V(g^{-1}) = \overline{\chi_V(g)}$$

The character is not necessarily a group homomorphism, because the trace of the product of two matrices is not necessarily the product of their traces. However, the following identity holds:

$$\chi_V(\phi(g)) = \chi_V(\phi(hgh^{-1}))$$

This is because $\phi(g)$ and $\phi(hgh^{-1})$ are similar, and similar matrices have the same trace. Thus, the character has constant value for all elements of G in the same conjugacy class, which makes the character function a class function on G. The fact that similar matrices have the same trace also means that isomorphic representations have the same characters.

Character theory is a very useful tool within representation theory. There is much more to say about characters, so much that unfortunately the author has run out of time to prove the following facts. The rest of this section will be devoted to stating interesting things about characters.

Proposition 6.2. *Over $\mathbb{C}$, two representations of a group G have the same characters if and only if they are isomorphic.*

Thus every representation is completely determined by its character. Recall that every representation of a finite group can be written as a direct sum of irreducible representations. If (V, ϕ) is a representation of G where $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$ with each W_i irreducible, then each matrix $\phi(g)$ is a block-diagonal matrix with each block corresponding to one of the W_is. Taking the trace of such a matrix, we have the identity

$$\chi_V = \chi_{W_1} + \chi_{W_2} + \cdots + \chi_{W_k}.$$

The following statements use an inner product defined on the space of complex class functions of G:

$$\langle \chi_V, \chi_W \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)\overline{\chi_W(g)}$$

Theorem 6.3 (First Orthogonality Relation)**.** *If (V, ϕ) and (W, ϕ') are irreducible, then the following holds:*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & (V,\phi) \text{ and } (W,\phi') \text{ are isomorphic} \\ 0 & (V,\phi) \text{ and } (W,\phi') \text{ are not isomorphic} \end{cases}$$

Theorem 6.4 (Irreducibility Criterion)**.** *(V, ϕ) is irreducible if and only if $\langle \chi_V, \chi_V \rangle = 1$.*

Characters are thus an extremely useful tool for determining irreducibility.

Theorem 6.5 (Completeness of Characters)**.** *The set of irreducible characters of G form a basis for the space of complex-valued class functions of G.*

Combining this with the orthogonality relation, we see that the irreducible characters of G form an orthogonal basis for the space of class functions of G.

Theorem 6.6 (Second Orthogonality Relation)**.** *Let G be a finite group and g be an element in the conjugacy class C. Then, summing over the distinct irreducible representations of G, we have*

$$\sum_{(V,\phi)} \chi_V(g)\overline{\chi_V(h)} = \begin{cases} 1 & h \in C \\ 0 & \text{otherwise} \end{cases}$$

7. Burnside's Theorem

Burnside's Theorem [1] says that every group of order $p^a q^b$, $a, b \neq 0$, is solvable. There is an extremely difficult proof of it using purely group theory, but using characters we'll be able to prove it in about two pages. Our proof will follow the one given in [2]. First, a few observations.

Proposition 7.1. *Every nontrivial representation (V, ϕ) of a simple group G is injective.*

If $\ker(\phi)$ was nontrivial, then G would have a normal subgroup, and that's not allowed, so $\ker(\phi) = \{e\}$.

Proposition 7.2. *If there is a $g \in G, g \neq e$ such that $\phi(g)$ is a scalar, then G is not simple.*

If $\phi(g)$ acts as a scalar, say $\phi(g)v = \lambda v$, then it commutes with $\phi(h)$ for all $h \in G$ because by properties of linear transformations $\phi(h)\lambda v = \lambda\phi(h)v$. So, either g is central, implying that $Z(G)$ is nontrivial so G has a nontrivial normal subgroup, or $g \in \ker(\phi)$, implying that ϕ is not injective. Either way, G cannot be simple.

Proposition 7.3. *$\phi(g)$ acts as a scalar if and only if $|\chi_V(g)| = \chi_V(e)$.*

If $\phi(g)$ is a scalar, then (since $\phi(g)$ must have roots of unity for eigenvalues) there is some root of unity ζ such that $\phi(g) = \zeta I$. Thus

$$\chi_V(g) = |\mathrm{Tr}(\zeta I)| = |\zeta| \,\mathrm{Tr}(I) = 1 \cdot \dim(V) = \chi_V(e).$$

Before we are ready for the next step of the proof, we take a detour to talk about algebraic integers.

Definition 7.4. *A complex number α is an algebraic number if it is a root of a monic polynomial with coefficients in $\mathbb{Q}$.*

Definition 7.5. *A complex number α is an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$.*

The algebraic integers, denoted by $\mathbb{A}$, are a ring. $\mathbb{A}$ is closed under addition, subtraction, and multiplication. A few examples of what $\mathbb{A}$ contains are the integers, roots of unity, nth roots of integers, and any sum or product of such numbers. $\mathbb{A}$ does not contain any element of $\mathbb{Q} \setminus \mathbb{Z}$. Another important property is that α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has all integer coefficients.

Proposition 7.6. *Let G be a finite group, C be some conjugacy class of G, and (V, ϕ) be an irreducible representation of G with character χ_V. Then $\chi_V(g) \in \mathbb{A}$ and $|C|\frac{\chi_V(C)}{\chi_V(e)} \in \mathbb{A}$.*

Since it's a sum of roots of unity, $\chi_V(g) \in \mathbb{A}$. Unfortunately the proof of the second part is beyond the scope of this paper.

Lemma 7.7. *If $|G| = p^a q^b$ with representation (ϕ, V), then there exists an irreducible character χ_V and an element g such that $\frac{\chi_V(g)}{\chi(e)}$ is a nonzero algebraic integer.*

Proof. The first thing we will need is a conjugacy class C of G whose order is a power of p. Let K be a Sylow q-subgroup of G. Since every p-group has a nontrivial center, let $g \in Z(K)$. Consider the group action of conjugation from G to itself. The stabilizer of g, which is $G_g = \{h \in G : hgh^{-1} = g\}$, contains K, so $[G : G_g]$ is a power of p. The orbit of g, which is $\mathcal{O}(g) = \{hgh^{-1} : h \in G\}$, is also the conjugacy class C of g. By the orbit-stabilizer theorem,

$$|\mathcal{O}(g)| = [G : G_g]$$

which means the order of C is a power of p. Next we need a χ_V such that $p \nmid \chi_V(e)$ and $\chi_V(C) \neq 0$. We can find this using the second orthogonality relation. Noting that $\overline{\chi_V(e)} = \chi_V(e)$, we can say

$$1 + \sum_{\chi_V} \chi_V(C)\chi_V(e) = 0$$

where C is the conjugacy class we just found and χ_V ranges over all characters of irreducible representations except the trivial one (that's where the 1 comes from). By Proposition 7.6, each $\chi_V(C)$ is an algebraic integer. If every $\chi_V(e)$ for which $\chi_V(C) \neq 0$ was divisible by p, then we could divide by p to get

$$-\frac{1}{p} = \sum_{\chi_V} \chi_V(C)\frac{\chi_V(e)}{p}.$$

But that expresses $\frac{1}{p}$ as a sum of algebraic integers when $\frac{1}{p}$ is not itself an algebraic integer. Therefore, for one of the χ_Vs for which $\chi_V(C) \neq 0$, we also have $p \nmid \chi_V(e)$. Now we are ready to put the lemma together.

By Proposition 7.6, $|C|\frac{\chi_V(C)}{\chi_V(e)}$ is an algebraic integer. Note that both $|C|$ and $\chi_V(e)$ are integers, and $\chi_V(C)$ is an algebraic integer. We spent all that time finding C and χ_V so that we could use the fact that $\gcd(|C|, \chi_V(e)) = 1$. By Bezout's Theorem, there exist integers m and n such that

$$m|C| + n\chi_V(e) = 1.$$

Multiply by $\frac{\chi_V(C)}{\chi_V(e)}$ to get

$$m|C|\frac{\chi_V(C)}{\chi_V(e)} + n\chi_V(C) = \frac{\chi_V(C)}{\chi_V(e)}.$$

We have just expressed $\frac{\chi_V(C)}{\chi_V(e)}$ as a sum of algebraic integers, so for any $g \in C$, $\frac{\chi_V(g)}{\chi_V(e)}$ is a nonzero algebraic integer. □

Lemma 7.8. *If χ_V is a character of the representation (V, ϕ) of G such that for some $g \in G$, $\frac{\chi_V(g)}{\chi_V(e)}$ is a nonzero algebraic integer, then $|\chi_V(g)| = \chi_V(e)$.*

Proof. Let $\dim V = n$. By Proposition 3.1, let the eigenvalues of $\phi(g)$ be roots of unity given by $e_1, \ldots, e_n$. Then let

$$\alpha = \frac{\chi_V(g)}{\chi_V(e)} = \frac{e_1 + e_2 + \cdots + e_n}{n}$$

We are interested in the minimal polynomial $p(x)$ of α in the field extension $\mathbb{C}/\mathbb{Q}$. We know $p(x)$ has rational coefficients and is irreducible. Now, suppose α is an algebraic integer. That implies

$p(x)$ has integer coefficients. The roots of $p(x)$ are the set $S = \{\sigma(\alpha) : \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})\}$. Any automorphism of $\mathbb{C}/\mathbb{Q}$ sends a root of unity to another root of unity, so every $\beta \in S$ is of the form

$$\frac{e_1 + e_2 + \cdots + e_n}{n}$$

for some roots of unity $e_1, \ldots e_n$. The maximum absolute value of this expression is 1, which occurs when $e_1 = e_2 = \cdots = e_n$. Therefore, for every $\beta \in S$, $|\beta| \leq 1$, implying that $\left|\prod_{\beta \in S} \beta\right|$ is at most 1. Since $\prod_{\beta \in S} \beta$ is the constant term of $p(x)$, it must be a nonzero integer if we wish α to be an algebraic integer. Thus, $\left|\prod_{\beta \in S} \beta\right|$ is exactly 1, which forces that for each $\beta \in S$, $|\beta| = 1$. Since $\alpha \in S$, $|\alpha| = \left|\frac{\chi_V(g)}{\chi_V(e)}\right| = 1$, which means $|\chi_V(g)| = \chi_V(e)$, as desired. □

Now we may prove the theorem.

Theorem 7.9 (Burnside's Theorem)**.** *Every group of order $p^a q^b$ with $a, b > 0$ is solvable.*

Proof. By Lemma 7.7, if $|G| = p^a q^b$, then it has an irreducible representation (V, ϕ) with a character χ_V such that for some $g \in G$, $\frac{\chi_V(g)}{\chi_V(e)}$ is an algebraic integer. By Lemma 7.8, since $\frac{\chi_V(g)}{\chi_V(e)}$ is an algebraic integer, $|\chi_V(g)| = \chi_V(e)$. Proposition 7.3 says that since $|\chi_V(g)| = \chi_V(e)$, $\phi(g)$ acts as a scalar, and Proposition 7.2 says that since $\phi(g)$ acts as a scalar, G cannot be simple. □

References

[1] W. Burnside. "On groups of order $p^\alpha q^\beta$". In: *Proceedings of the London Mathematical Society* S2-1.1 (Jan. 1904), pp. 388–392.

[2] C. Teleman. *Representation Theory*. Lecture notes, University of California Berkeley, pp. 40-42. 2005. URL: `https://math.berkeley.edu/~teleman/math/RepThry.pdf`.