MAT3116/3196: Linear Representations of Groups Vers. 0.90

Josef Lauri©
University of Malta

Contents

1 Preliminaries

This is an undergraduate short introduction to linear representations of finite groups. Therefore we shall only be able to scratch the surface of the subject. However, we shall do enough to see some spectacular results which can be achieved when power group theory and linear algebra are combined. These notes are intended to accompany the course which is built around the first eighteen chapters of *Representations and Characters of Groups* by Gordon James and Martin Liebeck, henceforth referred to as [JL]. Your are expected to have a copy of this book and to have it with you during the lectures, especially during the problem-solving sessions. In these notes, most theorems are presented with a reference to their numbering in [JL]. However, we do differ in some of the proofs which we present and in the order in which some results are presented. This is where these notes should be useful. Where we differ from [JL] we generally follow the first chapter of *The Symmetric Group* by Bruce Sagan, referred to as [S]. Your are not expected to have a copy of [S].

One important point to emphasise here is the notation for functions. In order to be consistent with [JL] we write functions as $(x)f$ rather than $f(x)$. This notation is not entirely consistent with other ways of representing functions. For example, we still write

$$f : A \to B$$

rather than

$$B \leftarrow A : f$$

and, in the cycle notation for permutations, $(xyz\ldots)$ still means that x is mapped into y rather than y into x. Later on in these notes (as in [JL]) we shall revert to the usage $f(x)$ for certain types of functions (notably, characters). All this might be a little confusing for those who are used to the notation "$f(x)$", but you will soon get used to it and we shall see that the use of both the left and the right sides of "x" for functions makes the presentation of some results flow more easily.

We differ from [JL] however in writing $f : x \mapsto x^2$, say, rather than $f : x \to x^2$, as [JL] does.

Finally, you should read Chapter 1 of [JL] which is a quick revision of elementary group theory.

2 Vector spaces and linear transformations

Please read Chapter 2 of [JL] which is a quick revision. In this sections we shall emphasise some salient points and notation.

Remember that a linear transformation

$$\theta : V \to W$$

is such that

$$(u + v)\theta = u\theta + v\theta$$

and

$$(\lambda v)\theta = \lambda(v\theta)$$

or, in one single condition,

$$(\lambda u + \mu v)\theta = \lambda(u\theta) + \mu(v\theta).$$

Recall also the relation

$$\dim V = \dim(\ker \theta) + \dim(\text{im } \theta).$$

2.1 Matrix representations of endomorphism

An *endomorphism* is a linear transformation a the vector space into itself.

A matrix is a coordinisation of a linear transformation, that is, way of representing a linear transformation with respect to a basis. Let θ be an endomorphism on the vector space V. Fix an *ordered basis* $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ of V. Then, for all i,

$$v_i\theta = \alpha_{i1}v_1 + \alpha_{i2}v_2 + \ldots + \alpha_{in}v_n.$$

The $n \times n$ matrix $(\alpha_{ij}$ is called the *matrix representation of* θ *with respect to the ordered basis* $\mathcal{B}$ and is denoted by

$$[\theta]_{\mathcal{B}}.$$

(All of this is under the assumption of a ground field F which, for us, will usually be $\mathbb{C}$. We us the term *matrix over* F if we want to emphasise that the entries in the matrix are from F.)

If θ and ϕ are emdomorphisms on V and $\lambda \in F$, then $\theta + \phi$, $\theta\phi$ (composition) and $\lambda\theta$ can be defined as endomorphisms on V by

$$v(\theta + \phi) = v\theta + v\phi$$

$$v(\theta\phi) = (v\theta)\phi$$
$$v(\lambda\theta) = \lambda(v\theta).$$

The nice thing about matrix representations of endomorphisms is that the usual rules for matrix multiplication, addition, and multiplication by a scalar is consistent with the above, that is,

$$[\theta + \phi]_{\mathcal{B}} = [\theta]_{\mathcal{B}} + [\phi]_{\mathcal{B}}$$
$$[\theta\phi]_{\mathcal{B}} = [\theta]_{\mathcal{B}}[\phi]_{\mathcal{B}}$$
$$[\lambda\theta]_{\mathcal{B}} = \lambda[\theta]_{\mathcal{B}}.$$

Note that although [JL] does not use this, we can extend this notation to vectors. That is, let $v \in V$ and let

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n.$$

Then we can write $[v]_{\mathcal{B}}$ to denote the n-tuple

$$(v_1, v_2, \ldots, v_n)$$

and it follows that, again using the usual multiplication of a matrix by a row vector,

$$[v\theta]_{\mathcal{B}} = [v]_{\mathcal{B}}[\theta]_{\mathcal{B}}.$$

The process of getting a matrix from an endomorphism can be reversed. Let A be an $n \times n$ matrix and V an n-dimensional vector, both over F. Fix an ordered basis $\mathcal{B}$. For any $v \in V$, compute $[v]_{\mathcal{B}}A$ and use the resulting row vector to form a linear combination of the ordered basis. Let this new vector be w that is, $[w]_{\mathcal{B}} = [v]_{\mathcal{B}}A$. Then $v \mapsto w$ is an endomorphism on V.

2.2 Change of basis

Consider the two ordered bases

$$\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$$

and

$$\mathcal{B}' = \{v'_1, v'_2, \ldots, v'_n\}.$$

Then

$$v'_i = t_{i1} + t_{i2} + \ldots + t_{in}v_n$$

for some elements t_{ij} in the field.

Let $T = (t_{ij}$. Then T is an invertible matrix which is called the *change of basis matrix* from $\mathcal{B}$ to $\mathcal{B}'$. The following result is important: Let θ be an endomorphism on V. Then

$$[\theta]_{\mathcal{B}} = T^{-1}[\theta]_{\mathcal{B}'}T.$$

2.3 Eigenvalues

Let θ be an endomorphism on V. Then $\lambda \in F$ is called an eigenvalue of θ with corresponding eigenvector $v \neq 0$ if

$$v\theta = \lambda v.$$

The scalar λ is an eigenvalue for θ iff

$$\det([\theta]_{\mathcal{B}} - \lambda I_n) = 0.$$

When $F = \mathbb{C}$, every endomorphism has an eigenvalue.

2.4 Direct sums

If $V_1, V_2, \ldots, V_r$ are subspaces of the vector space V and any $v \in V$ can be written uniquely as

$$v = v_1 + v_2 + \ldots + v_r$$

where $v_i \in V_i$, then V is said to be the *direct sum* of $V_1, V_2, \ldots, V_r$ and we write

$$V_1 \oplus V_2 \oplus \ldots \oplus V_r.$$

Example 2.1 *It is easy to write a vector space V as the direct sum of subspaces. Let $v_1, v_2, \ldots, v_k$ be linearly independent in V and let $U = sp(v_1, \ldots, v_k)$. Extend this to a basis*

$$v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$$

of V. Let $W = sp(v_{n+1}, \ldots, v_n)$. Then

$$V = U \oplus W.$$

The ease with which this can be done for a vector space is emphasised here because we will soon meet vector spaces with additional structures in which this cannot be done so easily.

Example 2.2 *If $V = U + W$ and $U \cap W = \{0\}$, then $V = U \oplus W$. Compare all this with the direct product of groups.*

2.5 Projections

If $V = U \oplus W$, define the endomorphisms π_1, π_2 on V by

$$v\pi_1 = (u + w)\pi_1 = u$$

and

$$v\pi_2 = (u + w)\pi_2 = w.$$

Then, im $\pi_1 = U$, $\ker \pi_1 = W$, and $\pi_1^2 = \pi$, and similarly for π_2. Conversely, an endomorphism π on V is a projection if $\pi^2 = \pi$, and it is always true that if π is a projection on V, then

$$V = \text{im } \pi \oplus \ker \pi.$$

2.6 Inner products

One main difference between the course and [JL] is the proof of Maschke's Theorem. The proof in the course uses inner products which we therefore have to introduce much earlier than [JL] does.

The motivation behind the general definition of inner products is the familiar scalar product or "dot" product of n-tuples. That is, let $u = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and $v = (\beta_1, \beta_2, \dots, \beta_n)$, where the entries are elements of $\mathbb{C}$. Then the dot product $u \cdot v$ is defined by

$$u \cdot v = \alpha_1 \overline{\beta_1} + \dots + \alpha_n \overline{\beta_n}.$$

Now this product satisfies a few basic properties which become the defining axioms of an inner product. That is, let V be a vector space over the field $\mathbb{C}$. With every pair of vectors $u, v \in V$ we associate a complex number $\langle u, v \rangle$ such that

1. $\langle u, v \rangle = \overline{\langle v, u \rangle}$;
2. $\langle \lambda_1 u_1 + \lambda_2 u_2, v \rangle = \lambda_1 \langle u_1, v \rangle + \lambda_2 \langle u_2, v \rangle$;
3. $\langle u, u \rangle > 0$ if $u \neq 0$.

Note that it follows that

$$\langle u, \lambda_1 v_1 + \lambda_2 v_2 \rangle = \overline{\lambda_1} \langle u, v_1 \rangle + \overline{\lambda_2} \langle u, v_2 \rangle.$$

Example 2.3 *One important vector space will arise as follows. Let A be a finite set (usually A will be a group). Let V be the space of all functions from A to $\mathbb{C}$. Therefore $(\theta + \phi)$ would be defined by*

$$(\theta + \phi)(a) = \theta(a) + \phi(a).$$

(Note that in this context, like [JL] we operate with functions on the left.)

Define $\langle \theta, \phi \rangle$ by

$$\langle \theta, \phi \rangle = \sum_{a \in A} \theta(a)\overline{\phi(a)}.$$

It is easy to verify that this satisfies the properties of an inner product.

An inner product provides us with another easy way of decomposing a vector space as a direct product of two subspaces. Two vectors u, v are said to be *orthogonal* with respect to an inner product if $\langle u, v \rangle = 0$. Let V be a vector space equipped with an inner product $\langle \cdot, \cdot \rangle$. Let U be a subspace of V. The *orthogonal complement* $U^\perp$ of U is the space

$$\{v \in V : \langle v, w \rangle = 0 \forall w \in U\}.$$

It is easy to check that

$$V = U \oplus U^\perp.$$

Again we must emphasise that we shall soon encounter vector spaces with more algebraic structure which are not so easy to decompose into direct sums.

2.7 Unitary transformations

A linear transformation $\theta : V \to V$ is said to be *unitary* (with respect to a given inner product $\langle \cdot, \cdot \rangle$) if, for all $u, v \in V$,

$$\langle u\theta, v\theta \rangle = \langle u, v \rangle.$$

Therefore a unitary transformation is one that preserves "distances", for example, a rotation. The following are standard results about unitary transformations.

1. θ is unitary iff it maps an orthonormal basis into an orthonormal basis.

2. Let $A = [\theta]_{\mathcal{B}}$ where $\mathcal{B}$ is an orthonormal basis. Then

   $$A^{-1} = \overline{A}^t.$$

   Conversely, if $A^{-1} = \overline{A}^t$ then A represents a unitary transformation with respect to some orthonormal basis. Such a matrix A is called *unitary*.

3. A unitary matrix has all columns (rows) orthonormal under the usual dot product of n-tuples.

3 A different look at an algebraic construction

Let G be an abelian group with operation denoted by $+$. Suppose there is an action of G on itself,

$$\hat{r} : g \mapsto \hat{r}g.$$

Since an action is a homomorphism,

$$\widehat{rs}g = \hat{r}\hat{s}(g).$$

Suppose we also insist that $\hat{r}$ is a homomorphism on G. Then,

$$\hat{r}(g + h) \mapsto \hat{r}g + \hat{r}h.$$

Suppose there is another action of G on itself. To show that this is a different action we shall act on the right. (This is one advantage of being open minded as to which side a function acts from: you have two sides to choose from.) So we have

$$\hat{r} : g \mapsto g\hat{r}$$

with

$$\widehat{rs} : g \mapsto g\hat{r}\hat{s}.$$

Suppose we also insist that

$$(g + h)\hat{r} = g\hat{r} + g\hat{s}.$$

Finally, suppose that, as we usually do, we shall remove the ˆ in order to simplify the notation. Look at all the above relations. What have we obtained? It is clear that we have a ring. What is the point of constructing a ring this way? What I want to point out here is that an abelian group with two appropriate actions gives rise to a new algebraic construct—a ring. This is something which will be central in our course and which you might need to make some effort to get used to. Namely, we shall have a homomorphism from a group G to a group of matrices and, if the resulting operations are viewed in a certain way, we end up with a new algebraic construct which will be called a module. You might want to look back at this section when we come to that point.

4 Group representations

We shall denote by $GL(n, F)$ the group of all invertible $n \times n$ matrices over a field F. A *representation* of G (*over* F) is a homomorphism

$$\rho : G \to GL(n, F)$$

for some n. The *degree* of the representation ρ is n.

Therefore, if $g \in G$, $(g)\rho$ (or $g\rho$, for short) is an $n \times n$ matrix over F. Also,

$$(gh)\rho = (g\rho)(h\rho)$$

where the multiplication between g and h is the group multiplication, but the multiplication between $g\rho$ and $h\rho$ is matrix multiplication.

Remember also that

$$1\rho = I_n$$

and

$$g^{-1}\rho = (g\rho)^{-1}.$$

Example 4.1 *Let*

$$D_4 = \langle a, b : a^4 = 1 = b^2, ab = ba^{-1} \rangle.$$

(Careful! [JL] denotes the dihedral group by D_8.) Let

$$\rho : a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and

$$\rho : b \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then, knowing what ρ does to the two generators, and using the fact that ρ is a homomorphism, we can write down $g\rho$ for any element g in G. Do it!

Example 4.2 *For any G and any n, $\rho : G \to GL(n, F)$ defined by $g\rho = I_n$ is a representation.*

Let ρ and σ be two representations over F of degree n. If there exists an invertible matrix T such that, **for all** $g \in G$,

$$g\sigma = T^{-1}(g\rho)T,$$

then ρ and σ are said to be *equivalent representations*.

Example 4.3 *Let ρ be the above representation of D_4. Let*

$$T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

therefore

$$T^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}.$$

Then,

$$a\sigma = T^{-1} a\rho T = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

and

$$b\sigma = T^{-1} b\rho T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Example 4.4 *Let $G = \mathbb{Z}_2 = \langle a : a^2 = 1 \rangle$ and define ρ by*

$$a\rho = \begin{pmatrix} 5 & 12 \\ -2 & 5 \end{pmatrix}.$$

Check that ρ is, in fact, a representation. (What do you need to check? Why is it sufficient to give the value of ρ on a?) Then, if T is as in the previous example,

$$a\sigma = T^{-1} a\rho T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

is an equivalent representation.

Given a representation $\rho : G \to GL(n, F)$, define

$$\ker \rho = \{g \in G : g\rho = I_n\}.$$

If $\ker \rho = G$ and $n = 1$, then $g\rho = 1$ for all $g \in G$. This is called the *trivial representation* of G.

If $\ker \rho = \{1\}$ then ρ is injective and $\mathrm{im}\ \rho \simeq G$. In this case ρ is said to be a *faithful representation.*

The above representations of D_4 are all faithful. Representations equivalent to faithful representations are faithful.

Finally, we shall often be faced with the following situation: as in Example 4.1, we are given a group G presented in terms of generators and relations and we are given, for each generator only, a matrix to which that generator corresponds. We extend this to a matrix representation of all of G in the obvious way using the generators. (For example, if g and h are two generators with corresponding matrices $g\rho$ and $h\rho$ and s is the element g^2h^{-1}, then $s\rho$ is defined to be $(g\rho)^2(h\rho)^{-1}$.) To verify that this assignment of matrices is indeed a representation (that is, a homomorphism) what we need to check is that the matrices assigned to the generators satisfy the corresponding relations satisfied by the generators. This is worked out in detail for the dihedral group and the symmetric group S_5 in Examples 1.4 and 1.5 in [JL].

Homework: Chapter 3 of [JL], numbers 2 and 5.

5 FG-Modules

(You might want to look back at the section where we discussed an alternative way of constructing rings.)

Let ρ be a representation of G, $\rho : G \to GL(n, F)$. Recall that the group $GL(n, F)$ can be seen as linear transformations of some vector space over F of dimension n. Therefore, although we do not mention this vector space explicitly, whenever we are faced with a representation of a group G, we have three algebraic spaces, G which acts on $GL(n, F)$ which in turn acts on a vector space. Let us now bring this vector space into the picture.

Let V be a vector space over F of dimension n. Let us in fact take $V = F^n$. (We could take any vector space over F of dimension n, take an ordered basis of the vector space and, for any vector, work with its components with respect to the basis.) Then matrix $g\rho$ acts on any $v \in V$ by matrix multiplication:

$$v \mapsto v(g\rho).$$

Let us simply denote $v(g\rho)$ by vg (this is similar to removing the ˆ in an action). Then it is clear that we have relations like

$$(\lambda v)g = \lambda(vg)$$

and

$$(u + v)g = ug + vg.$$

These are just consequences of matrix multiplication. But notice that, if we forget for a moment that g is in fact a shorthand for the matrix $g\rho$, it seems as if we are getting a new algebraic construct. (Compare with our construction of rings, above.) This motivates the following definition.

Let V be a vector space over F and let G be a group. Then V is said to be an *FG-module* if there is a multiplication vg ($v \in V, g \in G$) satisfying the following conditions for all $u, v \in V, \lambda \in F, g, h \in G$.

1. $vg \in V$
2. $v(gh) = (vg)h$
3. $v1 = v$
4. $(\lambda v)g = \lambda(vg)$
5. $(u+v)g = ug_v g$.

Note that property 2 gives that G is acting on V from the right, the fact that V is a vector space means that F is acting on V from the left (explaining why "FG''-module and properties 4 and 5 give that $v \mapsto vg$ is a linear transformation on V.

We have seen that a representation of G of order n turns $V = F^n$ into an FG-module (Theorem 4.4(1) in [JL]). It is important that you also realise that the converse is true, that is, a vector space of dimension n which is also an FG-module corresponds to a representation of G of degree n, as follows (this is Theorem 4.4(2) in [JL]).

Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be an ordered basis for V. Let

$$v_i g = \sum_j \alpha_{ij} v_j.$$

(Note, in the FG-module, vg is not the result of a matrix multiplication. It is just an element of v satisfying the axioms. It is up to us to turn it into a matrix, as we now do. The axioms are designed to ensure that the construction does yield a representation.)

Let $[g]_{\mathcal{B}}$ denote the matrix (α_{ij}). Then, if

$$v = \sum_i \beta_i v_i$$

, that is,

$$[v]_{\mathcal{B}} = [\beta_1, \ldots, \beta_n],$$

the mapping $v \mapsto vg$ corresponds to

$$[\beta_1, \ldots, \beta_n] \mapsto [\beta_1, \ldots, \beta_n][g]_{\mathcal{B}}.$$

Moreover, the axioms of the FG-module guarantee that the mapping

$$\rho : g \mapsto [g]_{\mathcal{B}}$$

is, in fact, a representation. (All of this is proved in detail in Theorem 4.4 of [JL].) What you need to understand and practice is the actual construction of the representation from a given FG-module. See examples 1 and 2 of section 4.5 of [JL].

A final note. We shall often be faced with the following situation. We are given a group G and a vector space V with a basis $\{v_1, \ldots, v_n\}$. We define a product $vg, v \in V, g \in G$ by defining the values of $v_i g$ only, and extending this to all elements of V by linearity (that is, if $v = \sum \lambda_i v_i$ then $vg = (\sum \lambda_i v_i)g = \sum \lambda_i (v_i g))$. It is easy to see, and it is proved in Proposition 4.6 in [JL], that for this product to give an FG-module what is required is that

1. $v_i \in V$;
2. $v_i(gh) = (v_i g)h$;
3. $v_i 1 = v_1$.

6 Equivalent representations and FG-modules

Given an FG-module V we can take any basis of V to give a representation following the above method. So does an FG-module correspond to essentially different representations? The answer is no, because the different representations arising from different choices of basis for V are all equivalent. This is the substance of Theorem 4.12 of [JL]. (Results like these give us confidence that our definitions of equivalent representations and FG-modules and our way of associating a representation with an FG-module are working they way we would expect them to do.)

We can summarise this theorem and its proof as follows.

1. Let V be an FG-module with basis $\mathcal{B}$ and let ρ be the corresponding representation, that is, $g\rho$ is equal to the matrix $[g]_{\mathcal{B}}$, as above.

   Suppose we take a different basis $\mathcal{B}'$ giving us the corresponding representation $\phi : g \mapsto [g]_{\mathcal{B}'}$.

   Let T be the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$. Then

$$[g]_{\mathcal{B}} = T^{-1}[g]_{\mathcal{B}'}T.$$

2. Let V be an FG-module with basis $\mathcal{B}$ and let ρ be the corresponding representation, that is, $g\rho$ is equal to the matrix $[g]_{\mathcal{B}}$, as above. Suppose σ is a representation of G, equivalent to ρ.

   Then there is a basis $\mathcal{B}''$ of V such that the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}''$ is R and

$$[g]_{\mathcal{B}} = R^{-1}[g]_{\mathcal{B}''}R.$$

That is, there is a basis $\mathcal{B}''$ of V such that $g\sigma = [g]_{\mathcal{B}''}$.

Example 6.1 *This is example 4.13 in [JL]. Let* $G = \mathbb{Z}_3 = C_3 = \langle a : a^3 = 1 \rangle$. *Let the representation* ρ *be defined by*

$$1\rho = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$a\rho = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

and

$$a^2\rho = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

(What do you need to check to verify that this is really a representation?)

Let $V = \mathbb{C}^2$. *We shall now turn* V *into a* $\mathbb{C}G$*-module as described above. Let* $v_1 = (1, 0)$ *and* $v_2 = (0, 1)$ *and let* $\mathcal{B} = \{v_1, v_2\}$ *be a basis for* V. *Turn* V *into a* $\mathbb{C}G$*-module by defining*

$$v_1 1 = v_1, v_2 1 = v_2,$$

$$v_1 a = v_2, v_2 a = -v_1 - v_2,$$

and

$$v_1 a^2 = -v_1 - v_2, v_2 a^2 = v_1,$$

and extending the action of G *on all of* V *by linearity. This turns* V *into a* $\mathbb{C}G$*-module. (How were the above values for* $v_i g, g \in G$ *obtained? What is the connection with the representation* ρ*?)*

Now let us take a different basis $\mathcal{B}' = \{u_1, u_2\}$ *of* V *where* $u_1 = v_1$ *and* $u_2 = v_1 + v_2$. *Then, from the definition of the product on the* $\mathbb{C}G$*-module* V *as defined above, we get (no matrices required here!)*

$$u_1 1 = u_1, u_2 1 = u_2,$$

$$u_1 a = -u_1 + u_2, u_2 a = -u_1,$$

and

$$u_1 a^2 = -u_2, u_2 a^2 = u_1 - u_2.$$

This gives the matrix representation $\phi : g \mapsto [g]_{\mathcal{B}'}$ *where*

$$[1]_{\mathcal{B}'} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$[a]_{\mathcal{B}'} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

and

$$[a^2]_{\mathcal{B}'} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Observe that the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$ is

$$T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

and in fact it can be checked that

$$[g]_{\mathcal{B}} = T^{-1}[g]_{\mathcal{B}'T}.$$

Homework: Chapter 4 exercise 3 of [JL]

7 Reducibility

Let V be an FG-module. W is said to be an *FG-submodule* of V if W is a subspace (as a vector space) of V and W is itself an FG-module, that is,

$$wg \in W \forall w \in W.$$

An FG-submodule is therefore a subspace of V which, moreover, is *invariant* under the action of G, that is, the action of G sends elements of W into W.

Clearly, $\{0\}$ and V are FG-submodules of V. These are called the *trivial submodules*. We now have this very important definition.

An FG-module V is *irreducible* iff the only submodules of V are the trivial ones. Otherwise V is called *reducible*.

It is important to appreciate this. For a vector space V it is easy to find non-trivial subspaces: any set of linearly independent vectors span a subspace. Therefore a vector space is never irreducible, unless it has dimension 1. But if V is moreover an FG-module, a subspace is not necessarily an FG-submodule because it might not be invariant under the action of G. It is, in general, less easy to find FG-submodules and it could happen that there are none, that is, the FG-module is irreducible.

Remember that with an FG-module is associated a representation of G and vice-versa. The above definition of an irreducible FG-module leads to the following definition.

A representation of G is said to be an *irreducible representation* (written *irrep* for short) if the corresponding FG-module $V = F^n$ is irreducible. Otherwise it is called *reducible*.

Now, we know what an irreducible FG-module means: it has no invariant subspaces. But what does an irrep mean in terms of matrices? We shall now investigate this question

Let V be an reducible FG-module and W an FG-submodule of V. Let $\dim W = k$, $0 < k < \dim V$. Let $\mathcal{B}_1$ be a basis for W. Extend $\mathcal{B}_1$ to $\mathcal{B}$, a basis for V. Then, for any $g \in G$, the matrix $[g]_{\mathcal{B}}$ has the form

$$\left(\begin{array}{c|c} X_g & 0 \\ \hline Y_g & Z_g \end{array}\right)$$

where X_g is a $k \times k$ matrix.

Conversely, a representation of G is reducible if it is equivalent to a representation of the above form.

Note that in this case,

$$[g]\mathcal{B}^r = \left(\begin{array}{c|c} X_g^r & 0 \\ \hline ? & Z_g^r \end{array}\right).$$

Also, $g \mapsto X_g$ and $g \mapsto Z_g$ are themselves representation of G. We shall soon have more to say about the possibility of making Y_g equal to the zero matrix.

Example 7.1 *Examples 5.2 and 5.5(1) in [JL].*

Let $G = C_3 = \langle a : a^3 = 1 \langle$, and let V be a vector space with basis $\{v_1, v_2, v_3\}$ We now turn V into an FG-module by defining an action of G on the basis. We must have that

$$v_1 1 = v_1, v_2 1 = v_2, v_3 1 = v_3.$$

We define the action of a by

$$v_1 a = v_2, v_2 a = v_3, v_3 a = v_1.$$

We therefore must have (why?)

$$v_1 a = v_3, v_2 a = v_1, v_3 a = v_2.$$

We shall show that this is a reducible FG-module. Let $w = v_1 + v_2 + v_3$ and let $W = sp(w)$. That is, W is a 1-dimensional subspace of V. It is easy to check that $w1 = wa = wa^2 = w$ therefore W is invariant under the action of G, that is, W is an FG-submodule.

But let $U = sp(z)$ where $z = v_1 + v_2$. Clearly U is a subspace (as vector space) of V but $za = (v_1 + v_2)a = v_2 + v_3$ which is not in U. Therefore U is not an FG-submodule.

Now, let $\mathcal{B}$ be the basis $\{v_1 + v_2 + v_3, v_1, v_2\}$ of V. (We are here extending a basis for W to a basis for V.) Then, check that

$$[1]_{\mathcal{B}} = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right),$$

$$[a]_{\mathcal{B}} = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & 1 \\ 1 & -1 & -1 \end{array}\right)$$

and

$$[a^2]_{\mathcal{B}} = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 1 & -1 & -1 \\ 0 & 1 & 0 \end{array}\right).$$

Note that the top left matrices give the 1-dimensional representation mapping all group elements into 1. This corresponds to the FG-submodule W. The bottom right matrices give the representation

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, a^2 \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

To what FG-module does this representation correspond? We shall have more to say about this question.

Example 7.2 *Example 5.5(2) in [JL].*

Let

$$G = D_4 = \langle a, b : a^4 = b^2 = 1, ab = ba^{-1} \rangle.$$

Let the representation ρ be defined by

$$a\rho = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b\rho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(Why is this a representation?)

Let $V = F^2$ ($F = \mathbb{R}$ or $F = \mathbb{C}$). We now turn V into an FG-module in the usual way. Define vg to be $v(g\rho)$. For example,

$$(1, 0)a = (1, 0) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (0, 1).$$

Therefore if $v = (1,0)$ *and* $w = (0,1)$, *the* FG*-module is defined by the rules*

$$va = w, wa = -v$$

and

$$vb = v, wb = -w,$$

by the above presentation for G, *and by linear extension. Therefore the action of* G *on* V *becomes,*

$$(\lambda, \mu)a = (-\mu, \lambda)$$

and

$$(\lambda, \mu)b = (\lambda, -\mu).$$

We now claim that this FG*-module (and hence the representation) is irreducible. Suppose* U *is a submodule of* V, $U \neq V$. *Therefore* $\dim U \leq 1$. *Therefore*

$$U = sp\{(\alpha, \beta)\}$$

for some fixed α, β *in* F. *Therefore*

$$(\alpha, \beta)a = (-\beta, \alpha) = h(\alpha, \beta),$$

and this forces $\alpha = \beta = 0$, *therefore* $U = \{(0,0)\}$, *that is, trivial. Hence* V *is irreducible, as claimed.*

Homework: Chapter 5 of [JL] number 1.

8 Maschke's Theorem

8.1 Reducibility for vector spaces does not work for FG-modules

Let us review the problem at hand. Any vector space V is reducible (that is, has a non-trivial subspace), unless it is 1-dimensional. Just take a set of linearly independent vectors whose size is less than the dimension of V and let W be the subspace spanned by these vectors. Moreover it is also easy to write V as the direct sum of two subspaces. Let $\{w_1, \ldots, w_k\}$ be the basis of W. Extend it to a basis $\{w_1, \ldots, w_k, w_{k+1}, \ldots, w_n\}$ of V and let W' be the subspace spanned by $\{w_{k+1}, \ldots, w_n\}$. Then

$$V = W \oplus W'.$$

If V is equipped with an inner product, then we have another way of writing V as a direct sum. Just let $W^{\perp}$ be the orthogonal complement of W and then

$$V = W \oplus W^{\perp}.$$

However, these simple constructions do not work when V is an FG-module. Firstly, W need not be an FG-submodule. That is, W need not be invariant under the action of G, that is, there could be some $w \in W$ such that wg is not in W. Secondly, even if W were to be an FG-submodule, there is no guarantee that W' or $W^{\perp}$ is an FG-submodule. (Therefore, these constructions can still be carried out in an FG-module which is, remember, also a vector space. But they yield sub-vector-spaces not necessarily FG-submodules.)

8.2 Decomposability of an FG-module

If an FG-module is not only reducible (has an FG-submodule) but can also be written as the direct product of two FG-submodules, we say that it is *decomposable* (this term is not defined in [JL]). Why would we want an FG-module to be decomposable? Recall the following: Let V be an reducible FG-module and W an FG-submodule of V. Let $\dim W = k$, $0 < k < \dim V$. Let $\mathcal{B}_1$ be a basis for W. Extend $\mathcal{B}_1$ to $\mathcal{B}$, a basis for V. Then, for any $g \in G$, the matrix $[g]_{\mathcal{B}}$ has the form

$$\left(\begin{array}{c|c} X_g & 0 \\ \hline Y_g & Z_g \end{array}\right)$$

where X_g is a $k \times k$ matrix. Here, if W' is the subspace spanned by the extra vectors in the basis $\mathcal{B}$, then $V = W \oplus W'$ as subspaces but not as FG-submodules. But if W' did happen to be an FG-submodule, that is invariant under the action of G, then for any $g \in G$, the matrix $[g]_{\mathcal{B}}$ has the form

$$\left(\begin{array}{c|c} X_g & 0 \\ \hline 0 & Z_g \end{array}\right).$$

(Why is this so?) This is quite a simplification of the matrix. For example, we would now have,

$$[g]\mathcal{B}^r = \left(\begin{array}{c|c} X_g^r & 0 \\ \hline 0 & Z_g^r \end{array}\right),$$

where we have removed the "question mark" which we had earlier. Moreover if W and W' were also decomposable, then we could transform the matrix representation further into a block diagonal form. If the reducible

FG-submodules encountered this way are always decomposable, then this simplification can go on until the blocks of the matrix correspond to irreducible FG-submodules. This way, any representation can be written in terms of irreducible ones, and the study of group representations essentially becomes the study of irreducible representations.

But for this programme to succeed we require decomposability of reducible representations. We shall see that, over the fields $\mathbb{R}$ or $\mathbb{C}$, all reducible FG-modules (and hence reducible representations) are decomposable.

8.3 The Theorem

Lemma 8.1 *Let V be an FG-module, U a submodule of V, and $\langle \cdot, \cdot \rangle$ an inner product on V which is invariant under the action of G, that is, $\langle ug, vg \rangle = \langle u, v \rangle$ for all $u, v \in V, g \in G$.*

Then $U^\perp$ is also an FG-submodule of V, and therefore $V = U \oplus U^\perp$ as FG-modules.

Proof. We are required to prove that

$$\forall g \in G, \forall w \in U^\perp, wg \in U^\perp.$$

Let $u \in U$. Then

$$\begin{aligned} \langle wg, u \rangle &= \langle wgg^{-1}, ug^{-1} \rangle \rangle \\ &= \langle w, ug^{-1} \rangle \\ &= 0 \end{aligned}$$

(The first step follows since the inner product is invariant under the action of G, and the last step follows since $w \in U^\perp$ and ug^{-1} is in U because U is an FG-submodule.)

Therefore wg is orthogonal to any $u \in U$, therefore $wg \in U^\perp$. □

We can now prove our first major theorem.

Theorem 8.1 (Maschke's Theorem) *Let G be a finite group and let F be $\mathbb{C}$ or $\mathbb{R}$. Let V be a reducible FG-module. Then V is decomposable. That is, let U be an FG-submodule of V. Then there is an FG-submodule W of V such that*

$$V = U \oplus W.$$

Proof. [This proof is given in [JL] as Exercise 6 at the end of Chapter 8.]

Pick any basis $\{v_1, \ldots, v_n\}$ of V. Consider the unique inner product that satisfies

$$\langle v_i, v_j \rangle = \delta_{ij}$$

extended to all of G by linearity. This inner product might not be G-invariant. Define

$$\langle v, w \rangle_1 = \sum_{g \in G} \langle vg, wg \rangle.$$

Then $\langle \cdot, \cdot \rangle_1$ satisfies the axioms of an inner product (exercise!).

Now,

$$\begin{aligned} \langle vh, wh \rangle_1 &= \sum_{g \in G} \langle vgh, wgh \rangle \\ &= \sum_{f \in G} \langle vf, wf \rangle \\ &= \langle v, w \rangle_1 \end{aligned}$$

that is, $\langle \cdot, \cdot \rangle_1$ is G-invariant.

Therefore, by the previous lemma, $W = U^{\perp}$ (where orthogonality is with respect to $\langle \cdot, \cdot \rangle_1$) is an FG-submodule, that is, $V = W \oplus W$ as submodules. □

Corollary 8.2 *Let V be an FG-module, where F is $\mathbb{R}$ or $\mathbb{C}$. Then V is the direct sum of irreducible submodules:*

$$V = U_1 \oplus U_2 \oplus \ldots U_r.$$

Proof. By induction on dimensions of U and W of Maschke's Theorem. □

An FG-module which is the direct sum of irreducible representations is called *completely reducible*. Therefore, as an immediate corollary of Maschke's Theorem we have that, if $F = \mathbb{C}$ or $\mathbb{R}$, every FG-module is completely reducible. Maschke's Theorem and its Corollary are therefore saying that, for the field $\mathbb{C}$, the notions of decomposable and completely irreducible coincide.

It is important to be able to interpret Maschke's Theorem in terms of matrix representations. So we now give this formally.

Theorem 8.3 (The corollary of Maschke's Theorem for Matrix Representations) *Let G be a finite group, $F = \mathbb{R}$ or $\mathbb{C}$, and ρ a representation of G of dimension $n > 0$. Then there is a basis over which all the matrices $g\rho$ are of the* *form*

$$X_g = \begin{pmatrix} X_g^1 & & & \\ & X_g^2 & & \\ & & \ddots & \\ & & & X_g^r \end{pmatrix}.$$

Proof. Let $V = F^n$. Let

$$vg := v(g\rho).$$

As usual, this turns V into an FG-module and, by the corollary to Maschke's Theorem,

$$V = U_1 \oplus \ldots \oplus U_r$$

with each U_i irreducible. Take an ordered basis $\mathcal{B}$ for V in which first come a basis for U_1, then a basis for U_2, etc/ With respect to this basis, each $[g\rho]_{\mathcal{B}}$ has the required form.

In fact, let T be the matrix that transforms from the standard basis of F^n to $\mathcal{B}$. Then

$$[g\rho]_{\mathcal{B}} = T^{-1}(g\rho)T,$$

that is, **one** matrix T block-diagonalises **all** matrices $g\rho$ **simultaneously**. □

A matrix of the form

$$\begin{pmatrix} X_1^g & & & \\ & X_2^g & & \\ & & \ddots & \\ & & & X_r^g \end{pmatrix}$$

is said to be the *direct sum* of the submatrices $X_g^1, \ldots$ and we write

$$X_g = X_g^1 \oplus X_g^2 \oplus \ldots \oplus X_g^r.$$

Homework: [JL] Chapter 8 Nos 1, 4, 5.

8.4 Failure of the Theorem

Example 8.1 *This is Example 8.2(2) in [JL]. Let $G = C_p = \langle a : a^p = 1 \rangle$, p prime. Let $F = \mathbb{Z}_p$. Consider the representation*

$$a^j \mapsto \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix}, \quad 0 \le j \le p-1.$$

The corresponding FG-module is $V = sp\{v_1, v_2\}$ where $v_1 = (1,0)$ and $v_2 = (0,1)$ and

$$v_1 a^j = v_1, \quad v_2 a^j = j v_1 + v_2.$$

Then $sp\{v_1\}$ is an FG-submodule of V. But there is no FG-submodule W such that $V = U \oplus W$, since U is the only 1-dimensional FG-submodule of V.

So Maschke's Theorem can fail if the field is not $\mathbb{R}$ or $\mathbb{C}$.

Example 8.2 *Compare this example with Exercise 5 of Chapter 8 in [JL]. It shows that Maschke's Theorem can fail for infinite groups.*

Let G be the group $\mathbb{R}^+$ under multiplication. Let $F = \mathbb{C}$ and $V = \mathbb{C}^2$. Define the representation

$$x \mapsto \begin{pmatrix} 1 & 0 \\ \log x & 1 \end{pmatrix} = x\rho.$$

Let $U = \{(c, o) : c \in \mathbb{C}\}$. Then it is easy to see that U is an FG-submodule of V. If the representation is completely reducible then there must exits a matrix T such that

$$T^{-1} x\rho T = \begin{pmatrix} a_x & 0 \\ 0 & b_x \end{pmatrix}$$

for all $x \in \mathbb{R}^+$.

Therefore a_x, a_y are eigenvalues for $x\rho$, and these are both 1. But then

$$x\rho = T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} T^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which is a contradiction.

9 Schur's Lemma

First we need to consider FG-homomorphisms. This material corresponds to Chapter 7 of [JL].

9.1 FG-homomorphisms

Let V and W be FG-modules. A function $\theta : V \to W$ is said to be an FG-*homomorphism* if θ is a linear transformation and moreover, if $\theta : v \mapsto w$

then $\theta : vg \mapsto wg$, for all $v, w \in V$ and $g \in G$. That is θ *does to* vg *what* g *does to* $v\theta$. This can be written also as

$$(vg)\theta = (v\theta)g$$

and can also be viewed as saying that the two "functions" $g\theta$ and θg (acting on V from the right) are equal.

What is the analogue of FG-homomorphisms for representations? Let $\rho : G \to GL(n, F)$ be a representation of G. An $n \times n$ matrix A corresponds to an FG-homomorphism (and not just a linear transformation, which it always does) if

$$(g\rho)A = A(g\rho)$$

for all $g \in G$.

The proof of the following theorem is easy and can be found in [JL].

Theorem 9.1 *Let V, W be FG-modules and $\theta : V \to W$ an FG-homomorphism. Then $\ker\theta$ is an FG-submodule of V and im θ is an FG-submodule of W.*

Another definition: Suppose that the FG-homomorphism is also invertible, that is, it is injective and surjective. Then we say that it is an *FG-isomorphism*. In this case we also say that V and W are *isomorphic FG-modules*, written as $V \simeq W$.

The next theorem (proof in [JL]) shows that our definitions do what is expected of them.

Theorem 9.2 *Suppose that V, W are FG-modules with bases $\mathcal{B}$ and $\mathcal{B}'$ respectively. The $V \simeq W$ iff the representations $\rho : g \mapsto [g]_{\mathcal{B}}$ and $\sigma : g \mapsto [g]_{\mathcal{B}'}$ are equivalent.*

We can now give the main result of this section.

9.2 The Lemma

Theorem 9.3 (Schur's Lemma) *Let V and W be irreducible $\mathbb{C}G$-modules. Then*

- *If $\theta : V \to W$ is a $\mathbb{C}G$-homomorphism, then either θ is a $\mathbb{C}G$-isomorphism or $v\theta = 0$ for all $v \in V$;*
- *If $\theta : V \to V$ is a $\mathbb{C}G$-isomorphism, then θ is a scalar multiple of the identity endomorphism $1_V : v \mapsto v$.*

Before we give the proof of Schur's Lemma we give the equivalent formulation in terms of representations.

Theorem 9.4 (Schur's Lemma in terms of representations) *Let $\rho : G \to GL(n, \mathbb{C})$ and $\sigma : G \to GL(n, \mathbb{C})$ be two irreducible representations of G.*

- *Suppose there exists a matrix T such that $T(g\rho) = (g\sigma)T$ for all $g \in G$. Then either T is non-singular and therefore ρ and σ are equivalent, or else $T = 0$.*

- *Suppose that there exists a matrix T such that $T(g\rho) = (g\rho)T$ for all $g \in G$. Then $T = \lambda I$ for some $\lambda \in \mathbb{C}$.*

Proof of Theorem 9.3. For the first part, suppose that $v\theta \neq 0$ for some $v \in V$. Then im $\theta \neq \{0\}$. But im θ is a submodule of W, which is irreducible. Therefore im $\theta = W$. Also, $\ker\theta$ is a submodule of V and it is not equal to V, since $v\theta \neq 0$ for some $v \in V$. But V is irreducible, therefore $\ker\theta = 0$. Therefore θ is invertible, hence an isomorphism.

For the second part, let θ be an endomorphism of V. By standard linear algebra, θ has an eigenvalue λ. Therefore $\ker(\theta - \lambda 1_V) \neq 0$. Thus $\ker(\theta - \lambda 1_V)$ is a non-zero submodule of V, which is irreducible. Therefore $\ker(\theta - \lambda 1_V) = V$, that is, $v(\theta - \lambda 1_V) = 0$ for all $v \in V$, that is, $v\theta = v\lambda 1_V$ for all $v \in V$. □

Note how elegant this proof is. It is a basis-free proof about matrices which commute with matrices of irreducible representations. This is possible thanks to the module view of representations.

Note also that the converse of the second part of the theorem is also true (Proposition 9.2 in [JL]). Read this as an exercise.

Example 9.1 *This is Example 9.4(1) in [JL]. Let*

$$G = C_3 = \langle a : a^3 = 1 \rangle.$$

Let $\rho : G \to GL(2, \mathbb{C})$ be defined by

$$a\rho = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

It is clear that the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

commutes with $1\rho, a\rho$ and $a^2\rho$. (Why?) But this matrix is not diagonal, therefore the representation is reducible.

HW: Generalise the previous example to show that any k-dimensional, $k > 0$, representation of an abelian group is reducible, that is, the irreducible representations of an abelian group are all 1-dimensional. This anticipates a result which we will soon obtain.

Example 9.2 *This is Example 9.4(2) in [JL]. Let*

$$G = D_5 = \langle a, b : a^5 = b^2 = 1, ab = ba^{-1} \rangle.$$

Let $\omega = e^{2\pi i/5}$. *Then the following defines a representation* $\rho : G \to GL(2, \mathbb{C})$*:*

$$a\rho = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \qquad b\rho = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Suppose

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

commutes with both $a\rho$ *and* $b\rho$*. Then, commutation with* A *forces* $\beta = \gamma = 0$ *and commutation with* $b\rho$ *forces* $\alpha = \delta$*. Therefore by the converse of Schur,* ρ *is irreducible.*

9.3 Abelian groups

Theorem 9.5 *Let* G *be a finite abelian group. Then every irreducible* $\mathbb{C}G$*-module has dimension 1.*

Proof. We shall give two equivalent proofs of this, one in terms of matrices, and another in terms of modules. First the one involving matrices. This is the exercise following Example 9.1.

For contradiction, let ρ be an irrep k-dimensional representation of G, $k \geq 2$. If all the matrices $g\rho$ are diagonal then ρ is reducible. So suppose that some matrix $A = g\rho$ is not diagonal. Since G is abelian, A commutes with all the matrices $g\rho$, for all $g \in G$. But this contradicts Schur's Lemma.

And now for the second proof (as given in [JL]). Let V be an irreducible $\mathbb{C}G$-module. Let $x \in G$. Since G is abelian,

$$vgx = vxg$$

for all $g \in G, v \in V$. Therefore the mapping $v \mapsto vx$ is a $\mathbb{C}G$-homomorphism. Therefore it is a scalar multiple of the identity 1_V, say $\lambda_x 1_V$. Thus

$$vx = \lambda_x v$$

for all $v \in V$.

Therefore every subspace W of V is a $\mathbb{C}G$-submodule (because if $w \in W$, then $wx = \lambda_x w \in W$). But V is irreducible, therefore $\dim V = 1$ in order that it cannot have non-trivial subspaces which, as we have seen, would be submodules. □

Note that the converse of this theorem is also true (Proposition 9.18 in[JL]).

9.4 Diagonalisation

Let $H = \langle g \rangle$ be a cyclic group of order n. Let V be a nonzero $\mathbb{C}H$-module. Therefore V is the direct sum of irreducible submodules,

$$V = U_1 \oplus V_2 \oplus \ldots \oplus U_r.$$

But each U_i has dimension 1. Therefore let $U_i = \langle u_i \rangle$. Let $\omega = e^{2\pi i/n}$.

Now,

$$u_i g = \lambda_i u_i$$

since U_i is a $\mathbb{C}H$-module. But

$$u_i g^n = \lambda_i^n u_i = u_i 1 = u_i.$$

Therefore λ_i is an n-th root of unity, that is

$$u_i g = \omega^{m_i} u_i.$$

Hence, if $\mathcal{B}$ is the basis $u_1, u_2, \ldots, u_r$ of V, then

$$[g]_{\mathcal{B}} = \begin{pmatrix} \omega^{m_1} & & & \\ & \omega^{m_2} & & \\ & & \ddots & \\ & & & \omega^{m_r} \end{pmatrix}.$$

We therefore have the following.

Theorem 9.6 *Let G be a finite group and V a $\mathbb{C}G$-module. If $g \in G$ then there is a basis $\mathcal{B}$ of V such that the matrix $[g]_{\mathcal{B}}$ is diagonal. If g has order n, then the entries on the diagonal of $[g]_{\mathcal{B}}$ are the n-th roots of unity.*

Proof. Let $H = \langle g \rangle$. Since V is also a $\mathbb{C}H$-module, the result follows from the above. (Note that changing g here changes the subgroup H which can therefore change the basis $\mathcal{B}$.) □

HW: Do Exercise of Chapter 9 of [JL].

10 Conjugacy and conjugacy classes

Revise Chapter 12 of [JL], particularly the sections on conjugacy classes, conjugacy class sizes and normal subgroups.

11 Characters

11.1 Definitions and examples

Let A be an $n \times n$ matrix. Then the *trace* of A, denoted by tr A, is defined to be

$$\text{tr } A = \sum_i = 1^n A_{ii}.$$

These facts about the trace are all well-known:

- $\text{tr } (A + B) = \text{tr } A + \text{tr } B$;
- $\text{tr } (AB) = \text{tr } (BA)$;
- $\text{tr } (T^{-1}AT) = \text{tr } A$;
- But in general, $\text{tr } (AB) \neq \text{tr } (A)\text{tr } (B)$.

Now let V be a $\mathbb{C}G$-module with basis $\mathcal{B}$. Then the *character* of V is the function

$$\chi : G \to \mathbb{C}$$

defined by

$$\chi(g) = \text{tr } ([g]_{\mathcal{B}} \quad (g \in G).$$

If $\rho : G \to GL(nn, \mathbb{C})$ is a representation of G, then the character of the representation is defined to be

$$\chi(g) = \text{tr } (g\rho) \quad (g \in G).$$

Note that the character of a $\mathbb{C}G$-module is independent of the choice of basis, and the character of a representation is the same as the character of a corresponding $\mathbb{C}G$-module. Note also that we write characters as functions from the left, not from the right.

If χ is any function from G to $\mathbb{C}$ we say that χ is a character of G if it is the character of some $\mathbb{C}G$-module (equivalently, of some representation of G over $GL(n, \mathbb{C})$). The character χ is said to be reducible (irreducible) if the corresponding $\mathbb{C}G$-module (or the corresponding representation) is reducible (irreducible).

It is clear (Theorem 13.5(2) in [JL]) that if x and y are conjugate elements of G then, for any character χ,

$$\chi(x) = \chi(y).$$

(This is because similar matrices have the same trace.)

For basically the same reason, we have the following (Theorem 13.5(1) in [JL]).

Theorem 11.1 *Isomorphic $\mathbb{C}G$-modules have the same character. In terms of representations, this means that equivalent representations of G have the same character.*

Although the proof of this result is easy, we have singled it out as a theorem because one of the remarkable results that we shall soon prove is that the converse is also true!

Example 11.1 *Let*

$$G = D_4 = \langle a, b : a^4 = b^2 = 1, ab = ba^{-1} \rangle.$$

Define $\rho : G \to GL(2, \mathbb{C})$ by

$$a\rho = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and

$$b\rho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then the character of this representation is given by the following table (check that these values correspond to the matrix representation — the full example is Example 13.6(1) in [JL]).

g	1	a	a^2	a^3	b	ab	a^2b	a^3b
$\chi(g)$	2	0	−2	0	0	0	0	0

Example 11.2 *Let*

$$G = D_3 = \langle a, b : a^3 = b^3 = 1, ab = ba^{-1} \rangle$$

and let three representations be defined as follows

$$\rho_1 : a \mapsto (1), \rho_1 : b \mapsto (1)$$

$$\rho_2 : a \mapsto (1), \rho_2 : b \mapsto (-1)$$

and

$$\rho_3 : a \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \rho_3 : b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where $\omega = exp(2\pi i/3)$.

Then the three corresponding characters χ_1, χ_2 *and* χ_3 *are given in the following table.*

g	1	a	a^2	b	ab	a^2b
$\chi_1(g)$	1	1	1	1	1	1
$\chi_2(g)$	1	1	1	-1	-1	-1
$\chi_3(g)$	2	-1	-1	0	0	0

.

11.2 First results

The *degree* of a character is defined to be the dimension of the corresponding $\mathbb{C}G$-module, that is, the size of the corresponding matrix representation.

Theorem 11.2 (Prop 13.9 in [JL) *] Let χ be the character of a $\mathbb{C}G$-module V. Let $g \in G$ with $|g| = m$. Then*

1. $\chi(1) = \dim V$*;*
2. $\chi(g)$ *is equal to the sum of* m*th roots of unity;*
3. $\chi(g^{-1}) = \overline{\chi(g)}$*;*
4. *if* g *is conjugate to* g^{-1} *then* $\chi(g)$ *is real.*

Proof.

1. Let $n = \dim V$. For any basis $\mathcal{B}$, $[1]_{\mathcal{B}} = I_n$ therefore the trace eqials n, that is, $\chi(1) = n$.
2. By Theorem 9.6 there exists a basis $\mathcal{B}$ of V such that

$$[g]_{\mathcal{B}} = \begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix}.$$

Therefore $\chi(g) = \omega_1 + \ldots + \omega_n$.

3. We know that tr $[g^{-1}]_{\mathcal{B}} = \omega_1^{-1} + \ldots + \omega_n^{-1}$ since the matrix is diagonal. But $\omega_i^{-1} = \overline{\omega_i}$ because each ω is of the form $e^{i\theta}$, θ real, (modulus equals 1) and $(e^{i\theta})^{-1} = e^{-i\theta} = \overline{e^{i\theta}}$. Therefore
$$\chi(g^{-1}) = \overline{omega}_1 + \ldots + \overline{\omega}_n = \overline{\chi(g)}.$$
4. If g is conjugate to g^{-1} then
$$\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$$
therefore $\chi(g)$ is real.

□

Corollary 11.3 (Corollary 13.10 in [JL) *] Let χ be a character of G and let $|g| = 2, g \in G$. Then $\chi(g)$ is an integer and*
$$\chi(g) = \chi(1) \bmod 2,$$
that is, $\chi(g)$ and $\chi(1)$ are both odd or both even.

Proof. Read [JL] as exercise. □

Theorem 11.4 (Theorem 13.11 in [JL) *] Let $\rho : G \to GL(n, \mathbb{C})$ be a representation of G and let χ be the character of ρ. Then,*

1. For $g \in G$,
$$|\chi(g) = \chi(1) = n$$
if and only if
$$g\rho = \lambda I_n$$
for some $\lambda \in \mathbb{C}$. (Note that this is true for all bases.)

2.
$$\ker \rho = \{g \in G : \chi(g) = \chi(1) = n\}.$$

Proof. For the first part read [JL] as exercise. For the second part, let $g \in \ker \rho$. Then $g\rho = I_n$ therefore $\chi(g) = n = \chi(1)$. Conversely, let $\chi(g) = \chi(1)$. Therefore $g\rho = \lambda I_n$ for some $\lambda \in \mathbb{C}$, by the first part. Therefore $\chi(g) = \lambda n = \lambda\chi(1)$, hence $\lambda = 1$, that is, $g\rho = I_n$. Therefore $g \in \ker \rho$. □

The second part of this theorem justifies the following definition. Let χ be a character of G. Then the *kernel* of χ, $\ker \chi$, is defined by
$$\ker \chi = \{g \in G : \chi(g) = \chi(1) = n\}.$$
By the previous theorem, $\ker \rho = \ker \chi$, therefore $\ker \chi$ is a normal subgroup of G. We also say that the character χ is *faithful* if $\ker \chi = \{1\}$.

Theorem 11.5 (Proposition 13.15 in [JL]) *] Let χ be a character of G. Then $\overline{\chi}$ is a character of G. Also, if χ is irreducible then so is $\overline{\chi}$.*

Proof. Read from [JL] as exercise. □

Example 11.3 *Let*

$$G = D_3 = \langle a, b : a^3 = b^2 = 1, ab = ba^{-1} \rangle.$$

It will eventually be shown that the irreducible characters of G are χ_1, χ_2 and χ_3 which take on these values.

g	1	a	a^2	b	ab	a^2b
$\chi_1(g)$	1	1	1	1	1	1
$\chi_2(g)$	1	1	1	-1	-1	-1
$\chi_3(g)$	2	-1	-1	0	0	0

Note that $\ker \chi_1 = G$, $\ker \chi_2 = \langle a \rangle$ *and* $\ker \chi_3 = \{1\}$, *therefore χ_3 is faithful.*

Example 11.4 *Let*

$$G = D_4 = \{a, b : a^4 = b^2 = 1, ab = ba^{-1}\}$$

and let χ be as shown.

g	1	a	a^2	a^3	b	ab	a^2b	a^3b
$\chi(g)$	2	0	-2	0	0	0	0	0

It can be seen that chi is faithful, since $\ker \chi = \{1\}$. *Also, since* $|\chi(a^2)| = |-2| = \chi(1)|$ *it follows that if $\rho : G \to GL(2, \mathbb{C})$ is a representation with character χ then $a^2\rho = -I_n$, by the previous theorem.*

Look back at some of the homework examples which we have worked earlier out earlier and see how easier it is to tell that a representation is faithful just by reading off its character. It is remarkable that with so little information compared with the whole matrix of the representation we can still make conclusions about the nature of the representations. This is only the beginning. We shall soon see truly remarkable results which tell us that the trace, which seemingly throws away so much of the matrix, can tell us practically all we would want to know about the representation.

12 Orthogonality relations of the first kind

12.1 The relations

Recall that

$$\begin{aligned}\langle \chi, \psi \rangle &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} \\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\psi(g^{-1}).\end{aligned}$$

We extend this definition to arbitrary functions from G to $\mathbb{C}$, that is, for two such functions f and g their inner product $\langle f, h\rangle'$ is defined by

$$\langle f, g\rangle' = \frac{1}{|G|}\sum_{g\in G} f(g)h(g^{-1}).$$

Note that $\langle ., . \rangle$ and $\langle ., . \rangle$ are equal for characters.

It is mainly at this juncture that we part company, at least for the time being, with [JL]. The proof we give for the following theorem is very different from that in [JL]. The latter uses more the concept of FG-modules, while the one below involves working with matrices, summation over suffixes etc. The proof in [JL] is therefore more elegant and more in the tradition of the modern way of presenting group representations. However [JL]'s proof requires more preparation and I wanted to get quickly to the more important results. This way the student is not presented with a long sequence of abstract definitions and lemmas which do not seem to lead to concrete results about characters. Therefore from this point our sequencing of the results will also be quite different from that in [JL]. The proof we present here is quite standard (and clever) and can be found, for example, in Sagan [S]. [Hold on tight here. This is one of the difficult proofs in the course. There is no conceptual difficulty really. But there is the difficulty of having to check carefully some matrix manipulations.]

Theorem 12.1 (Theorem 1.9.3 in [S) *] Let χ and ψ be irreducible characters of a group G. Then*

$$\langle \chi, \psi \rangle = \delta_{\chi,\psi}.$$

Proof. Let χ, ψ be, respectively, characters of matrix representations A, B of degrees d, f. For any element $g \in G$ we write the corresponding matrix as $A(g)$ or $B(g)$.

Let $X = (x_{ij})$ be a $d \times f$ matrix of indeterminates x_{ij}. Let

$$Y = \frac{1}{|G|} \sum_{g \in G} A(g) X B(g^{-1}).$$

We claim that $A(h)Y = YB(h)$ for all $h \in G$. So, to prove the claim:

$$\begin{aligned} A(h)YB(h)^{-1} &= \frac{1}{|G|} \sum_{g \in G} A(h)A(g)XB(g^{-1})B(h^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} A(gh)XB((hg)^{-1}) \\ &= \frac{1}{|G|} \sum_{f \in G} A(f)XB(f^{-1}) \\ &= Y, \end{aligned}$$

as required.

Therefore, by Schur's Lemma,

$$Y = \begin{cases} 0 & \text{if } \ A \not\simeq B \\ cI_d & \text{if } \ A \simeq B \end{cases}.$$

Consider first the case when $\chi \neq \psi$, that is, $A \not\simeq B$. Therefore $y_{ij} = 0$ for all i, j. Therefore

$$\frac{1}{|G|} \sum_{k,l} \sum_{g} a_{ik}(g) x_{kl} b_{lj}(g^{-1}) = 0.$$

Equating coefficients of each x_{kl} to zero gives,

$$\frac{1}{|G|} \sum_{g} a_{ik}(g) b_{lj}(g^{-1}) = 0, \quad \forall i, j, k, l.$$

Therefore

$$\langle a_{ik}, b_{lj} \rangle' = 0, \quad \forall i, j, k, l.$$

Now,

$$\chi = \text{tr } A = a_{11} + a_{22} + \ldots + a_{dd}$$

and

$$\psi = \text{tr } B = b_{11} + b_{22} + \ldots + b_{ff}.$$

But

$$\langle \chi, \psi \rangle = \langle \chi, \psi \rangle' = \sum_{i,j} \langle a_{ii}, b_{jj} \langle' = 0,$$

as required.

Now let us suppose that $\chi = \psi$. We may therefore take $A = B$. As we have seen, there is a $c \in \mathbb{C}$ such that $y_{ij} = c\delta_{ij}$. Therefore, as above,

$$\langle a_{ik}, a_{lj} \rangle' = 0$$

as long as $i \neq j$. We need to consider what happens when $i = j$.

Let us start with

$$\frac{1}{|G|} \sum_{g \in G} A(g) X A(g^{-1}) = cI_d$$

and take traces. This gives

$$\begin{aligned} cd &= \text{tr } cI_d \\ &= \frac{1}{|G|} \sum_{g \in G} \text{tr } [A(g) X A(g^{-1})] \\ &= \frac{1}{|G|} \sum_{g \in G} \text{tr } X \\ &= \text{tr } X. \end{aligned}$$

Therefore $y_{ii} = c = \frac{1}{d} \text{tr } X$. That is,

$$y_{ii} = \frac{1}{|G|} \sum_{k,l} \sum_{g \in G} a_{ik}(g) x_{kl} a_{li}(g^{-1}) = \frac{1}{d}(x_{1,1} + x_{2,2} + \ldots + x_{d,d}).$$

Equating coefficients of like monomials gives

$$\begin{aligned} \langle a_{ik}, a_{li} \rangle' &= \frac{1}{|G|} \sum_{g \in G} a_{ik}(g) a_{li}(g^{-1}) \\ &= \frac{1}{d} \delta_{kl}. \end{aligned}$$

Therefore

$$\begin{aligned} \langle \chi, \chi \rangle &= \sum_{i,j=1}^{d} \langle a_{ii}, a_{jj} \rangle' \\ &= \sum_{i=1}^{d} \langle a_{ii}, a_{ii} \rangle' \\ &= \sum_{1}^{d} \frac{1}{d} \\ &= 1, \end{aligned}$$

as required. □

12.2 Consequences of the orthogonality relations

We can now easily obtain, as a corollary to the last theorem, some truly remarkable results on characters.

Theorem 12.2 *Let X be a matrix representation of G with character χ. Suppose*

$$X \simeq m_1 X_1 \oplus m_2 X_2 \oplus \ldots \oplus m_k X_k$$

where the X_i are pairwise non-equivalent irreps with characters χ_i. Then

1. $\chi = m_i \chi_1 + m_2 \chi_2 + \ldots m_k \chi_k$;
2. $\langle \chi, \chi_j \rangle = m_j, \forall j$;
3. $\langle \chi, \chi \rangle = m_1^2 + m_2^2 + \ldots + m_k^2$;
4. *X is irreducible iff $\langle \chi, \chi \rangle = 1$;*
5. *Let Y be another matrix representation of G with character ψ. Then $X \simeq Y$ iff $\chi(g) = \psi(g)$ for all $g \in G$.*

Proof.

1. $\chi = \text{tr } X = \text{tr } \oplus m_i X_i = \sum m_i \chi_i$.
2. $\langle \chi, \chi_j \rangle = \langle \sum_i m_i \chi_i, \chi_j \rangle = \sum_i m_i \langle \chi_i, \chi_j \rangle = m_j$, by the orthogonality relations.
3. $$\begin{aligned} \langle \chi, \chi \rangle &= \langle \sum_i m_i \chi_i, \sum_j m_j \chi_j \rangle \\ &= \sum_{i,j} m_i \overline{m}_j \langle \chi_i, \chi_j \rangle \\ &= \sum_i m_i^2, \end{aligned}$$

   again by orthogonality.
4. If χ is irreducible then all m_i are zero except one whose value equals 1. Therefore $\langle \chi, \chi \rangle = 1$ by the second result.

   Conversely, suppose $\langle \chi, \chi \rangle = 1 = \sum_i m_i^2$. Since the m_i are integers, all of them must be zero except one whose value should be 1. Therefore χ is irreducible.

5. We already know that if $X \simeq Y$ then, by elementary matrix algebra, $\chi = \psi$. For the converse, let

$$Y \simeq \oplus n_i X_i.$$

(If necessary let missing irreps have coefficient 0.) Since $\chi = \psi$, $\langle \chi, \chi_i \rangle = \langle \chi, \psi_i \rangle$ for all i. Therefore, by the second result, $m_i = n_i$ for all i. That is, $X \simeq Y$.

□

The last two parts of this theorem are truly remarkable results. You should now look back at some of the problems you did earlier and work them out using characters.

13 The group algebra

The previous result answered a number of important questions about representations of a group. However, we still have two very important questions to investigate: How many irreps does a finite group have? How do we find them?

To answer these questions we need to develop further some algebraic machinery. Now that we have some significant concrete results under our belts we can sit back and calmly develop some more abstract theory. Do not worry, concrete results will soon appear.

13.1 The definition of the group algebra $\mathbb{C}G$

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group. The field F will always be $\mathbb{C}$. The *group algebra* $\mathbb{C}G$ (or FG) is the set of all formal sums

$$\alpha_1 g_1 + \alpha_2 g_2 + \ldots + \alpha_n g_n$$

where each α_i is in $\mathbb{C}$. What do these formal sums mean?

For the moment think of $\mathbb{C}G$ as a vector space over $\mathbb{C}$. We can think of a vector over $\mathbb{C}$ as an ordered list of elements of $\mathbb{C}$. How do we denote the order of a list of complex numbers? We usually do this by fixing the actual order in which the numbers are written. For example, in the vector

$$v = (2, 0, -i, 7)$$

the number 0 is the second element in the list and the number $-i$ is the third. However, we could also indicate this order by using "markers". For example, we could write v as cubic polynomial:

$$2 - ix^2 + 7x^3.$$

Here, the marker x^i denotes the $i+1$-st position. The absence of the marker x means that its coefficient is 0, which is therefore the second element in the list. The term $-ix^2$ means that $-i$ is the third element in the list. We can write the above cubic as

$$-ix^2 + 7x^3 + 2$$

without disturbing the order of the list – the markers do that job for us.

Now, instead of the markers x^i we can use the elements of any finite set, including a group. For example, if the group G is the Klein 4-group

$$\{1, a, b, c\}$$

(remember, the elements commute, each of a, b, c has order 2, and $ab = c$, $ac = b$ and $bc = a$) we could decide that, as markers, the elements $1, a, b, c$ will denote, respectively, the first, second, third and fourth positions. Then, the vector v can be written as

$$2.1 - ib + 7c.$$

The group algebra $\mathbb{C}G$ would therefore be a 4-dimensional vector space isomorphic to $\mathbb{C}^4$ with $1, a, b, c$ as basis elements.

Therefore, up to this point, what we have is that the group algebra $\mathbb{C}G$ is an n-dimensional vector space over $\mathbb{C}$, where n is the order of G, with basis elements $g_1, g_2, \ldots, g_n$. This basis is called the *natural basis* of $\mathbb{C}G$. However, the markers we have chosen are not lifeless symbols. They belong to a group, and can therefore be multiplied. We can use this to put a multiplication on $\mathbb{C}G$. For example, in the 4-dimensional case we are using as an example, if w is the vector

$$2a + ic$$

then, in a natural way (letting the group multiplication be distributive over the addition in $\mathbb{C}G$) we can say that vw is equal to

$$4a + 2ic - 4ic + a + 14b + 7i$$

which, by collecting like terms, simplifies to

$$7i + 5a + 14b - 2ic.$$

In general, we are defining a product on $\mathbb{C}G$ such that

$$(\sum_g \lambda_g g)(\sum_h \mu_h h) = \sum_{g,h} \lambda_g \mu_h (gh).$$

This turns the vector space $\mathbb{C}G$ into what is called an *algebra*. $\mathbb{C}G$ is called an algebra because, apart from the axioms of a vector space, the above product satisfies, for all $r, s, t \in \mathbb{C}G$ and for all $\lambda \in \mathbb{C}$, the following properties:

1. $rs \in V$;
2. $r(st) = (rs)t$;
3. $r.1 = 1.r = r$ where 1 here denotes the identity element in G;
4. $(\lambda r)s = \lambda(rs) = r(\lambda s)$;
5. $(r + s)t = rt + st$;
6. $r(s + t) = rs + rt$;
7. $r0 = 0r = 0$ where 0 denotes the zero in $\mathbb{C}$.

13.2 The group algebra as a $\mathbb{C}G$-module: The regular $\mathbb{C}G$-module

Let us consider the vector space $V = \mathbb{C}G$. As a vector space we can turn this in the usual way into a $\mathbb{C}G$-module by defining a suitable action of G on V. The multiplicative structure of $\mathbb{C}G$ enables us to define this action in a very natural way because any given element $g \in G$ can be considered to be an element of $\mathbb{C}G$ (coefficient 1 for the element g and coefficients 0 for all the other elements) therefore the element g can be multiplied by any element in $\mathbb{C}G$ by virtue of the multiplication in $\mathbb{C}G$ which we have just defined.

Thus, we define the action $g : V \to V$ (remember $V = \mathbb{C}G$) by $g : v \mapsto vg$. This is called the *right regular representation* of G (Do you recall Cayley's Theorem?) and the resulting module is called the *regular* $\mathbb{C}G$-module. This module is faithful (that is, the only $g \in G$ for which $vg = v$ for all $v \in \mathbb{C}G$ is $g = 1$).

The corresponding matrix representation ρ (the regular representation – we drop the "right" for short) is defined by taking the natural basis $\mathcal{B}$ of $\mathbb{C}G$ and letting $g\rho$ be $[g]_{\mathcal{B}}$. An example should make all these concepts clear.

Example 13.1 *Let $G = C_3 = \langle a : a^3 = 1 \rangle$. Elements of $\mathbb{C}G$ therefore have the form $\lambda_1 1 + \lambda_2 a + \lambda_3 a^2$, $\lambda_i \in \mathbb{C}$. Consider the action on the natural basis $\mathcal{B} = \{1, a, a^2\}$ of $\mathbb{C}G$.*

$(1)1 = 1$, $(a)1 = a$ and $(a^2)1 = a^2$. Therefore

$$1\rho = [1]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

$(1)a = a$, $(a)a = a^2$ and $(a^2)a = 1$. Therefore

$$a\rho = [a]_{\mathcal{B}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

$(1)a^2 = a^2$, $(a)a^2 = 1$ and $(a^2)a^2 = a$. Therefore

$$a^2\rho = [a^2]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

13.3 The character of the regular $\mathbb{C}G$-module

Now that we have turned the group algebra $\mathbb{C}G$ into a $\mathbb{C}G$-module we can ask what its character is. This character is called the *regular character* of G and is denoted by χ_{reg}.

Theorem 13.1 *Let χ_{reg} be the regular character of G. Then*

$$\chi_{reg}(1) = |G|$$

and

$$\chi_{reg}(g) = 0$$

for all $g \neq 1$.

Proof. Let $\mathcal{B}$ be the basis $\{g_1, g_2, \ldots, g_n\}$ of $\mathbb{C}G$. By an earlier result, $\chi_{\text{reg}}(1) = \dim \mathbb{C}G = |G|$, as required. But we can also see this as follows: $[1]_{\mathcal{B}} = I_n$ since 1 sends every g_i onto itself. But the trace of I_n is $n = |G|$.

Now, let $g \in G, g \neq 1$. Then, for any g_i, $g_i g = g_j$ for some $j \neq i$. Therefore the i-th row of $[g]_{\mathcal{B}}$ has zero everywhere except for the column j which is not equal to i. In particular, the ii-th entry of $[g]_{\mathcal{B}}$ is 0. Therefore

$$\chi_{\text{reg}}(g) = \text{tr } [g]_{\mathcal{B}} = 0,$$

as required. □

(NOTE: This result and the form of the inner product on characters should remind you of "fixed points" and Burnside's Lemma.)

13.4 The group algebra can also act instead of the group G

When we have an FG-module V, the group G acts on the elements of V from the right. That is, for any elements $v \in V$ and $g \in G$ there is an element $vg \in V$. We shall sometimes extend this action so that not only do elements of G act on elements of V from the right but also elements of FG (which are linear combinations of elements of G) act on elements of V from the right. We define this action in a very natural way, that is, if V is an FG-module, $v \in V$ and $r \in FG$ such that $r = \sum_g \lambda_g g$, then the product vr is defined by

$$vr = \sum_{g \in G} \lambda_g (vg).$$

Note now the multiple use of "FG" or "$\mathbb{C}G$": (i) We write "FG-module" or "$\mathbb{C}G$-module" to denote a vector space over F or $\mathbb{C}$ on which the group G acts from the right; (ii) We write FG or $\mathbb{C}G$ to denote the group algebra whose elements are formal sums consisting of linear combinations (over F or $\mathbb{C}$) of elements of G — this structure is a vector space on which we have also defined a product; (iii) and now we see that the group algebra FG or $\mathbb{C}G$ can act from the right in place of G on a given FG-module or $\mathbb{C}G$module — the given module could be FG ($\mathbb{C}G$) itself!

Try to understand these uses of the symbol FG and do not be confused by them.

Homework: Exercises 1,2,3 and 6 from Chapter 6 of [JL].

13.5 $\mathbb{C}G$ is the mother of all representations

The following theorem shows why it is worth studying the group algebra $\mathbb{C}G$ as a $\mathbb{C}G$-module: it contains all irreducible $\mathbb{C}G$-modules of G! (In particular this shows that there are only a finite number of non-equivalent irreducible modules of a given finite group. Why?)

Theorem 13.2 *Let*

$$\mathbb{C}G = m_1 V_i \oplus m_2 V_2 \oplus \dots$$

as a $\mathbb{C}G$-module, where V_i are non-equivalent irreducible $\mathbb{C}G$-modules of G. (All possible irreducible $\mathbb{C}G$-modules are written down and those which do not appear in $\mathbb{C}G$ have the corresponding multiplicity m_i equal to 0. Of course, only a finite number of the m_i are non-zero since $\mathbb{C}G$ is finite-dimensional.)

Then, for all i, $m_i = V_i$. Therefore each irreducible V_i appears in $\mathbb{C}G$ at least once and there are therefore a finite number of them.

Proof. Let V_i have character χ_i. Then,

$$\begin{aligned} m_i &= \langle \chi_{\text{reg}}, \chi_i \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\text{reg}}(g) \chi(g^{-1}) \\ &= \frac{1}{|G|} \chi_{\text{reg}}(1) \chi_i(1) \\ &= \frac{|G|}{|G|} \dim V_i. \end{aligned}$$

We shall henceforth denote by k the number of irreducible $\mathbb{C}G$-modules (or representations over $\mathbb{C}$) of G. This result will also be useful.

Theorem 13.3 *Let $\mathbb{C}G$ be as above. Then*

$$sum_i^k (\dim V_i)^2 = |G|,$$

where the sum is taken over all non-equivalent irreducible $\mathbb{C}G$-modules of G.

Proof. Take dimensions in

$$\mathbb{C}G = m_1 V_i \oplus m_2 V_2 \oplus \ldots \oplus m_k V_k.$$

Then

$$\dim \mathbb{C}G = \dim(m_1 V_1) + \dim(m_2 V_2) + \ldots + \dim(m_k V_k)$$

therefore

$$\begin{aligned} |G| &= m_1 \dim V_1 + m_2 \dim V_2 + \ldots + m_k \dim V_k \\ &= \sum_i^k (\dim V_i)^2. \end{aligned}$$

This result can also be obtained from

$$\frac{|G|.|G|}{|G|} = \langle \chi_{\text{reg}}, \chi_{\text{reg}} \rangle = \sum m_i^2.$$

□

Example 13.2 *Let $G = D_3$. The complete list of characters is*

g	1	a	a^2	b	ab	a^2b
$\chi_1(g)$	1	1	1	1	1	1
$\chi_2(g)$	1	1	1	−1	−1	−1
$\chi_3(g)$	2	−1	−1	0	0	0

.

Verify some of the results we have proved on characters, such as $\langle \chi_i, \chi_j \rangle = \delta_{ij}$*. Also, note that the linear combination* $\chi_1 + \chi_2 + 2\chi_3$ *(coefficient of* χ_i *equal to the dimension of* χ_i*) takes the value 6 on* $1 \in G$ *and 0 on any* $g \neq 1$*, which is the regular character.*

14 The number of irreducible characters

14.1 Functions from G to $\mathbb{C}$ and class functions

¿From now on we shall denote the irreducible characters of G by

$$\chi_1, \chi_2, \ldots, \chi_k$$

now that we know that there is a finite number of them. Therefore k will denote the number of irreducible characters of G or, equivalently, the number of irreducible representations of G or, equivalently, the number of irreducible $\mathbb{C}G$-modules. For the next few pages we shall attack the problem of determining the value of k.

But before proceeding with this we take a short simple look at the set of all functions from G to $\mathbb{C}$. Characters are such functions, but we might need to widen our horizon to include other functions from G to $\mathbb{C}$.

The set of all functions $G \to \mathbb{C}$ can be turned into a vector space. Let $f, h : G \to \mathbb{C}$ and let $G = \{g_1, g_2, \ldots, g_n\}$. Then we can consider f (and similarly h) to be the n-tuple $(f(g_1), f(g_2), \ldots, f(g_n))$. Therefore the natural way to define addition of functions would be by

$$(f + h)(g_i) = f(g_i) + h(g_i)$$

and this would be analogous to the addition of n-tuples where

$$(f(g_1), f(g_2), \ldots, f(g_n)) + (h(g_1), h(g_2), \ldots, h(g_n))$$

becomes equal to

$$(f(g_1) + h(g_1), f(g_2) + h(g_2), \ldots, f(g_n) + h(g_n)).$$

Similarly multiplication by a scalar is defined by

$$(\lambda f)(g_i) = \lambda f(g_i).$$

With these definitions the set of all functions $G \to \mathbb{C}$ becomes a vector space. (Note the similarity of this idea with the turning of $\mathbb{C}G$ into a vector space by considering the g_i as place holders. After all, the function f for which

$f(g_i) = \lambda_i$ is another way of considering the element $\lambda_1 g_1 + \lambda_2 g_2 + \ldots + \lambda_n g_n$ of $\mathbb{C}G$. Note also that the way we have been representing characters—which are functions $G \to \mathbb{C}$—in a tabular form is again a way of considering each character as an n-tuple of complex numbers.)

What is the dimension of the space of all functions $G \to \mathbb{C}$? It is clearly $n = |G|$ because the functions $f_1, f_2, \ldots, f_n$ defined by

$$f_i(g) = \begin{cases} 1 & \text{if} \quad g = g_i \\ 0 & \text{if} \quad g \neq g_i \end{cases}.$$

form a basis.

We are however more interested in a particular subspace of the space of all functions $G \to \mathbb{C}$. A *class function* $\psi : g \to \mathbb{C}$ is a function which is constant on conjugacy classes of G, that is, it has the property that $\psi(x) = \psi(y)$ whenever x and y are conjugates in G. We shall denote the set of of class functions by $\mathcal{C}$. It is easy to see that $\mathcal{C}$ is a vector space under the above definition of addition of functions and scalar multiplication.

What is the dimension of $\mathcal{C}$? Let the conjugacy classes of G be $C_i, C_2, \ldots, C_l$ (from now on, l will denote the number of conjugacy classes of G). Let $\psi_1, \psi_2, \ldots, \psi_l$ be functions defined as follows

$$\psi_i(g) = \begin{cases} 1 & \text{if} \quad g \in C_i \\ 0 & \text{if} \quad g \notin C_i \end{cases}..$$

Then the ψ_i are clearly class functions. Also they are linearly independent. Moreover, they span $\mathcal{C}$ because if $\psi \in \mathcal{C}$ takes on the value λ_i on all elements of the class C_i, then

$$\psi = \lambda_1 \psi_1 + \lambda_2 \psi_2 + \ldots + \lambda_l \psi_l.$$

Therefore the $\psi_1, \psi_2, \ldots, \psi_l$ form a basis for $\mathcal{C}$ and hence the dimension of $\mathcal{C}$ is l, the number of conjugacy classes of G.

Now, characters are elements of $\mathcal{C}$ and the irreducible characters have a particular property.

Lemma 14.1 *The irreducible characters $\chi_1, \ldots, \chi_k$ of G are linearly independent.*

Proof. This again follows from the orthogonality properties of irreducible characters. For, let

$$\lambda_1 \chi_1 + \lambda_2 \chi_2 + \ldots + \lambda_l \chi_k = 0,$$

the zero function. Therefore

$$0 = \langle \lambda_1\chi_1 + \lambda_2\chi_2 + \ldots + \lambda_l\chi_k, \chi_i \rangle = \lambda_i,$$

and this is true for all λ_i. □

But the irreducible characters live in $\mathcal{C}$ which has dimension l. Therefore we immediately have,

Theorem 14.1 *Let k be the number of irreducible characters of G and let l be the number of conjugacy classes. Then*

$$k \leq l.$$

We have gone some way towards finding k: it is at most equal to the number of equivalence classes. Could it possibly be that $k = l$? We shall show that in fact this is the case by proving that $k \geq l$. But to do this we need to consider in more detail the internal structure of $\mathbb{C}G$.

14.2 $Z(\mathbb{C}G)$, the centre of $\mathbb{C}G$ and class sums

The centre of $\mathbb{C}G$, denoted by $Z(\mathbb{C}G)$, consists with all those elements of $\mathbb{C}G$ which commute with all other elements of $\mathbb{C}G$, that is

$$Z(\mathbb{C}G) = \{z \in \mathbb{C}G : zr = rz \forall r \in \mathbb{C}G\}.$$

Clearly, the centre of G, $Z(G)$, is in $\mathbb{C}G$, because any element z of $Z(G)$ can, like any other element of G, be considered an element of $\mathbb{C}G$ (z is that linear combination of elements of G in which every coefficient is 0 except the coefficient of z itself, which is 1). But then, for any $r = \sum_g \lambda_g g$ in $\mathbb{C}G$,

$$\begin{aligned} rz &= (\sum_g \lambda_g g)z \\ &= \sum_g \lambda_g g z \\ &= \sum_g \lambda_g z g \\ &= z(\sum_g \lambda_g g) \\ &= zr. \end{aligned}$$

However, in $\mathbb{C}G$ the centre can be much larger than just $Z(G)$, as the following example illustrates.

Example 14.1 *Let* $G = D_4 = \langle a, b : a^4 = b^2 = 1, ba = a^{-1}b\rangle$. *Then the conjugacy classes are*

$$\{1\}, \{a^2\}, \{a, a^3\}, \{b, a^2b\}, \{ab, a^3b\}.$$

We shall soon see that conjugacy classes are important when considering $\mathbb{C}G$.) *Let*

$$z = ia^2 + (2 + 3i)(b + a^2b).$$

You do check that for any $g \in G$, $zg = gz$. *(Check it only for* $g = a$ *and* $g = b$. *The rest follows since all other elements are generated by* a *and* b. *But DO IT! It will help you to understand better the sequel.) Then, since any elelemnt of* $\mathbb{C}G$ *is a linear combination of elements of* G *it follows that* $zr = rz$ *for all* $r \in \mathbb{C}G$.

Note that the centre of G *is trivial, so here we have an element of* $Z(\mathbb{C}G)$ *which is not obtained from any central element of* G.

Did you notice that the element z in the above example was a linear combination of elements of G with the property that elements in the same conjugacy class had the same coefficient? In this case the coefficients were i, $2 + 3i$ and 0. It will turn out that all elements of $Z(\mathbb{C}G)$ have to be of this form. Before we proof this we need another definition.

Let the classes of G be $C_1, \ldots, C_l$, as above. For each class C_i define the following element $\overline{C}_i$ of $\mathbb{C}G$:

$$\overline{C}_i = \sum_{g \in C_i} g.$$

Therefore in $\overline{C}_i$ all the elements of C_i have coefficient equal to 1 and all the others have coefficient equal to 0. Each $\overline{C}_i$ is called a class sum.

We are now ready to start proving some results. But note the state of play. On the one hand we have characters which are special (linearly independent) class functions, that is functions which are constant on conjugacy classes. On the other hand we have class sums, which are elements of $\mathbb{C}G$ whose coefficients are constant on conjugacy classes. If we can only put our fingers on the right buttons surely some connections will drop out.

First a technical lemma whish we shall soon be needing.

Lemma 14.2 (Theorem 9.14 in [JL) *.] Let* V *be an irreducible* $\mathbb{C}G$*-module and let* $z \in Z(\mathbb{C}G)$. *Then there exists* $\lambda \in \mathbb{C}$ *such that*

$$vz = \lambda v, \forall v \in V.$$

Proof. Note that the product vz involves $\mathbb{C}G$ acting on the left on the $\mathbb{C}G$-module V, an extension of the action of G on V which we pointed out in Section 13.4.

Now, for all $g \in G$ and for all $v \in V$,

$$vgz = vzg.$$

Therefore the map $v \mapsto vz$ is a $\mathbb{C}G$-homomorphism on V. But V is irreducible, therefore by Schur's Lemma this homomorphism is equal to

$$v \mapsto \lambda v$$

where λ is a constant depending only on z. □

The next theorem brings us closer to our goal of connecting the space generated by irreducible characters to the space generated by class sums, and hence connecting k with l.

Theorem 14.2 (Theorem 12.22 in [JL) *.] The class sums* $\overline{C}_1, \ldots, \overline{C}_l$ *form a basis for* $Z(\mathbb{C}G)$*. Hence* $\dim Z(\mathbb{C}G) = l$*.*

Proof. We present the proof in three parts.

Part 1: $\overline{C}_i \in Z(\mathbb{C}G)$
Write C_i in terms of conjugates of a single element g:

$$C_i = \{y_1^{-1} g y_1, y_2^{-1} g y_2, \ldots, y_r^{-1} g y_r\}.$$

Therefore

$$\overline{C}_i = y_1^{-1} g y_1 + y_2^{-1} g y_2 + \ldots + y_r^{-1} g y_r.$$

Therefore, for any $h \in G$,

$$h^{-1}\overline{C}_i h = (y_1 h)^{-1} g y_1 h + (y_2 h)^{-1} g y_2 h + \ldots + (y_r h)^{-1} g y_r h,$$

and this is still equal to $\overline{C}_i$ written in a possibly different order.

Therefore $\overline{C}_i h = h\overline{C}_i$, that is, $\overline{C}_i$ commutes with every element of G. But any element of $\mathbb{C}G$ is a linear combination of elements of G, therefore $\overline{C}_i$ commutes with every element of $\mathbb{C}G$.

Part 2: $\overline{C}_1, \ldots, \overline{C}_l$ *are linearly independent*
This is easy. Let

$$\lambda_1 \overline{C}_1 + \ldots + \lambda_l \overline{C}_l = 0.$$

But conjugacy classes are mutually disjoint, therefore $\lambda_i = 0$ for al i.

Part 3: $\overline{C}_1, \ldots, \overline{C}_l$ span $Z(\mathbb{C}G)$
This is equivalent to proving that any element of $Z(\mathbb{C}G)$ has constant coefficients on conjugacy classes. Let

$$r = \sum_g \lambda_g g \in Z(\mathbb{C}G).$$

For $h \in G$, $h^{-1}rh = r$. Therefore

$$\sum_g \lambda_g h^{-1} gh = \sum_g \lambda_g g.$$

If we look carefully at this we see that it means that, for any h, the coefficient of $h^{-1}gh$ in r is the same as the coefficient of g; that is, in the sum r, elements in the same conjugacy class must have the same coefficient. So, suppose that elements in class C_i have coefficient λ_i. It then follows that

$$r = \sum_1^l \lambda_i \overline{C}_i,$$

as required. □

We have finally arrived at our result. To prove this we shall bring to bear most of the facts we have obtained for $\mathbb{C}G$.

Theorem 14.3 (Theorem 15.3 in [JL) *.] The number of irreducible characters of G is equal to the number of conjugacy classes of G, that is, $k = l$.*

Proof. We have already shown that $k \leq l$. We now need to show that $l \leq k$.

Consider the regular $\mathbb{C}G$-module $V = \mathbb{C}G$. Let $V_1, \ldots V_k$ be a complete set of non-isomorphic irreducible $\mathbb{C}G$-modules. (Remember, by Theorem 13.2, all k irreducibles must appear as submodules of V.) Therefore

$$\mathbb{C}G = W_1 \oplus \ldots \oplus W_k$$

where each W_i is a direct sum of a number of copies of V_i. But $1 \in \mathbb{C}G$, therefore

$$1 = f_1 + f_2 + \ldots + f_k$$

where each f_i is in W_i (some of the f_i might be equal to 0).

Now let $z \in Z(\mathbb{C}G)$. By Lemma 14.2, for each i there exists a $\lambda_i \in \mathbb{C}$ such that, for all $v \in V_i$, $vz = \lambda_i v$. Therefore $wz = \lambda_i w$ for all $w \in W_i$. In particular, $f_i z = \lambda_i f_i$. Therefore

$$\begin{aligned} z &= 1z \\ &= (f_1 + f_2 + \ldots + f_k)z \\ &= \lambda_1 f_1 + \lambda_2 f_2 + \ldots + \lambda_k f_k. \end{aligned}$$

Therefore $Z(\mathbb{C}G)$ is contained in the subspace spanned by $f_1, f_2, \ldots, f_k$, which must therefore have dimension at most k. But we have seen that $\dim Z(\mathbb{C}G) = l$. Therefore $l \leq k$, as required. □

15 The character table and orthogonality relations of the second kind

From now on we shall present what is called the *character table* of G as follows. Each row of the table will represent an irreducible character of G. Therefore the table will contain k rows. By convention, the first row is taken to represent the trivial character, that is the character which takes on the value 1 for each element of G. Since characters are constant on conjugacy classes, we only need to know the values of a character on class. Therefore each column will represent a conjugacy class. The values in the i-the row and j-th column of the table will be the value which the i-th character takes on the elements in the j-th conjugacy class. Usually, at the head of the table we give a row which contains a representative from each class. Below this, I usually give the size of the class, which I find useful for calculating inner products. Note that [JL] and some other books give the centraliser of any element in the class. Since conjugacy is an action of G on itself, each conjugacy class is an orbit of this action, and the centraliser of an element is its stabiliser, it follows (from the Orbit-Stabiliser Theorem) that these sizes are related by

$$|G| = |C(g)| \cdot |C_i|,$$

where g is any element in the class C_i and $C(g)$ is its centraliser. Therefore knowing one number easily gives the other, but be careful whenever you read a character table which convention is used.

So, for example, the character table of $D_3 \simeq S_3$ which was given in

Example 11.2 in long form will now be written as

g	1	a	b
Size of class	1	2	3
$\chi_1(g)$	1	1	1
$\chi_2(g)$	1	1	-1
$\chi_3(g)$	2	-1	0

Therefore to compute the inner product $\langle \chi_1, \chi_2 \rangle$ from this table we have to compute

$$1 \times 1 \times 2 + 2 \times 1 \times -1 + 3 \times -1.$$

Do not forget the sizes of the classes! These are the *orthogonality relations of the first kind* or the *row orthogonality relations.*

Now, the fact that the character table is square will enable us to obtain easily the *column orthogonality relations* or the *orthogonality relations of the second kind* from the row orthogonality relations.

The row orthogonality relations give that

$$\langle \chi_r, \chi_s \rangle = \delta_{rs},$$

that is,

$$\frac{1}{|G|} \sum_{i=1}^{k} \chi_r(g_i)\overline{\chi_s(g_i)} \times |C_i| = \delta_{rs},$$

where g_i is any element in the class C_i.[1]

Now modify the character table by multiplying each entry $\chi_r(g_i)$ by

$$\sqrt{\frac{|C_i|}{|G|}}$$

and let M be the resulting matrix (sometimes called the *modified character table*). Therefore the rows of M are orthogonal, that is,

$$M\overline{M}^t = I$$

which implies that

$$\overline{M}^t M = I.$$

[1] We have two fixed characters and we are summing over all elements. The r and s refer to the two characters.

Therefore the columns of M are also orthogonal. This can be written as

$$\frac{|C_r|^{\frac{1}{2}}|C_r|^{\frac{1}{2}}}{|G|}\sum_{i=1}^{k}\chi_(g_r)\overline{\chi_i(g_s)} = \delta_{rs}.^2$$

When $r \neq s$, this sum is zero, that is,

$$\sum_{i=1}^{k}\chi_i(g_r)\overline{\chi_i(g_s)} = 0.$$

When $r = s$, these relations become

$$\frac{|C_r|}{|G|}\sum_{i=1}^{k}\chi_i(g_r)\overline{\chi_i(g_r)} = 1.$$

These relations can be written as

$$\sum_{\chi}\chi_{C_r}\cdot\overline{\chi_{C_s}} = \frac{|G|}{|C_r|}\delta_{rs}$$

or

$$\sum_{i=1}^{k}\chi_i(g_r)\overline{\chi_i(g_r)} = \frac{|G|}{|C_r|}\delta_{rs}.$$

Note that while the in the orthogonality relations of the second kind the factor $|C_i|$ can be taken outside the summation, in the relations of the first kind they have to remain under the sum. Also, remember that $\frac{|G|}{|C_r|}$ is equal to $|C(g_r)|$, the centraliser of any $g_r \in C_r$, and sometimes you can see the relations of the second kind written this way (e.g. in [JL]).

Example 15.1 *Let us look again at the character table of S_3 (this is the same group D_4 we had above, but let us treat it as if it were another group). Confirm that S_3 has three conjugacy classes (remember that two permutations are conjugate in S_3 iff they have the same cycle structure). One irreducible character is the trivial character. Another is the sign character, where $\chi(g)$ is 1 if g is an even permutation and $\chi(g)$ is -1 if g is an odd permutation (this is an irreducible character for every S_n). Therefore the character table of S_n can be written as*

g	id	$(12)(3)$	(123)
Size of class	1	3	2
$\chi_1(g)$	1	1	1
$\chi_2(g)$	1	-1	1
$\chi_3(g)$	x	y	z

,

[2] We now have two fixed elements and we sum over all characters. Here, r and s refer to the conjugacy classes of the two elements.

where x, y, z need to be found. Now,

$$1^2 + 1^2 + x^2 = |G| = 6$$

therefore $x = 2$. Also,

$$1.1 + 1.(-1) + 2y = 0$$

therefore $y = 0$, and

$$1.1 + 1.1 + 2z = 0$$

therefore $z = -1$. Therefore we have found the whole character table.

Note that we could have tried the inner product of the third column with itself to find z. This would have given us $z^2 = 1$ and we would have needed to decide which of $z = \pm 1$ is the correct answer. The advantage of doing the inner product of column 3 with column 1 is that it removes this problem. But note that is is no difficulty when we do the inner product of the first column with itself, because here all entries are dimensions therefore they are all positive integers.

HW.

1. Read Examples 14.18, 15.7, 16.3 and 16.5 in [JL].
2. Do Problems: Ch 15, nos 1,2,3 and Ch 16, nos 1,2,3,4 from [JL].

16 Defining representation for permutation groups

When G is a permutation group it has a very natural representation associated with its permutation action. Thus, let G be a subgroup of S_n. Let V be a vector space with basis $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$. Turn V into an FG-module by defining

$$v_i g = v_{ig}$$

and extending this definition to all of V by linearity.

Example 16.1 *This is Example 4.9 in [JL]. Let $G = S_4$ and let $\mathcal{B} = \{v_1, \ldots, v_4\}$. If $g = (12)$, then*

$$v_1 g = v_2, v_2 g = v_1, v_3 g = v_3, v_4 g = v_4$$

and if $h = (124)$, then

$$v_1 h = v_3, v_2 h = v_2, v_3 h = v_4, v_4 h = v_1.$$

Construct $[g]_{\mathcal{B}}$ and $[h]_{\mathcal{B}}$.

This module V is called the *permutation module* of G or the *defining module* of G. The basis $\{v_1, \ldots, v_n\}$ is the *natural basis* of V.

The matrices of this representation are permutation matrices, that is, they have a single 1 in every row and column and all the other entries are 0.

This module (representation) is faithful since only id fixes every v_i. By Cayley's Theorem, every finite group has a faithful representation of dimension $|G|$.

Example 16.2 *Let G be a subgroup of S_n and let $\{v_1, \ldots, v_n\}$ be the natural basis of the permutation module. Let $u = v_1 + \ldots + v_n$. Clearly $ug = u$ for all $g \in G$. Therefore $U = sp\{u\}$ is a non-trivial submodule of V, hence the permutation module is not irreducible.*

Example 16.3 *This is example 7.3(3) in [JL]. Let G be a subgroup of S_n and let $\{v_1, \ldots, v_n\}$ be the natural basis of the permutation module V. Let $W = sp\{w\}$ be the trivial module for G (that is, $wg = w$ for all $g \in G$).*

Define $\theta : V \to W$ by

$$\theta : \sum_1^n \lambda_i v_i \mapsto (\sum_1^n) w.$$

Therefore $v_i\theta = w$ for all i. Hence θ is a linear transformation. Also, you can easily check that $(vg)\theta = (v\theta)g$. Therefore θ is an FG-homomorphism, and

$$\ker\theta = \{\sum_1^n \lambda_i v_i : \sum_1^n \lambda_i = 0\}$$

is a submodule of V.

16.1 The permutation character and the standard character

The character of the permutation module is clearly

$$\chi(g) = \text{number of fixed points of the permutation } g = |\text{fix}(g)|.$$

This character is denoted in [JL] (Section 13.22) by π.

Example 16.4 *Let $G = S_4$. Then G has five conjugacy classes with representatives as shown in this table which also shows the permutation character.*

g	id	(12)	(123)	(12)(34)	(1234)
Size of class	1	6	8	3	6
$\pi(g)$	4	2	1	0	0

The permutation character leads to another character which is sometimes called the standard character and it is denote by ν in [JL]. It is defined as follows:

$$\nu = \pi - 1,$$

that is, $\nu(g) = |\text{fix}(g)| - 1$ for all $g \in G$.

But we still have not shown that this function $G \to \mathbb{C}$ is a character. Read the proof of this which is Proposition 13.24 in [JL]. The proof requires the result of Example 16.3.

Theorem 16.1 *The function defined by*

$$\nu = \pi - 1$$

is a character of G*.*

But we can say more. If the permutation group is 2-transitive (in particular, if it is S_n), then ν is irreducible. We state the result for S_n here as a theorem in order to be able to refer to it.

Theorem 16.2 *The standard character* ν *of* S_n *is an irreducible character.*

HW.

1. How much of the full character table of S_4 can you produce?

2. If π is the character of the permutation group G and it is written as a linear combination of irreducible characters of G, which coefficient gives the number of orbits of the action of G?

17 More on the character table: normal subgroups

We have now seen ways of constructing the full character table from partial information using inner products. With more sophisticated machinery one can of course do more. In fact character tables have been found of groups about which only very partial information was know. Chapter 17 of [JL] presents some of the more elementary of these methods. We review them here. In many cases you will not be required to reproduce the proofs, but you should know how the results are used in practice.

Character tables are very important because they tell us a lot about the group. Chapter 17 also looks at one aspect of this, namely, using the character table to determine whether a group is simple. So we look at some of these results concerning normal subgroups. Normal subgroups are also important for the other problem we have mentioned, that is, the problem of constructing the full character table of a group. So normal subgroups are the leitmotif of this chapter.

Unfortunately in my treatment I am going to change again the order of things from that given in Chapter 17 of [JL].

17.1 New irreducibles from products of old irreducibles

Let χ and λ be characters of G (in fact, for this definition, χ and λ can be any functions $g :\to F$). Then the product $\chi\lambda$ is defined by

$$\chi\lambda(g) = \chi(g)\lambda(g).$$

Now, even if χ and λ are irreducible characters, we do not have any guarantee that $\chi\lambda$ is a character, let alone that it is irreducible. However, if one of the characters is linear (dimension = 1) then we have the following simple result.

Theorem 17.1 (Theorem 17.14 in [JL) *.] Suppose that χ is a character of G and λ is a linear character of G. The the product $\chi\lambda$ is a character of G. Moreover, $\chi\lambda$ is irreducible iff χ is irreducible.*

Proof. Let $\rho : G \to GL(n, \mathbb{C})$ be a representation of G with character χ. Remember that the matrix representation with character λ is λ itself, because $\lambda(g)$ is simply a complex number. Define $\rho\lambda : G \to GL(n, \mathbb{C})$ by

$$g(\rho\lambda) = \lambda(g)(g\rho).$$

That is, $g(\rho\lambda)$ is just the matrix $g\rho$ multiplied by the complex number $\lambda(g)$. We first want to show that the function $\rho\lambda$ is a homomorphism. This is easy, because

$$\begin{aligned}(gh)(\rho\lambda) &= \lambda(gh)((gh)\rho) \\ &= \lambda(g)\lambda(h)g\rho h\rho \\ &= (\lambda(g)g\rho)(\lambda(h)h\rho) \\ &= (g\rho\lambda)(h\rho\lambda)\end{aligned}$$

But the matrix $g(\rho\lambda)$ has trace $\lambda(g)$tr $(g\rho)$ which is equal to $\lambda(g)$
$chi(g)$. Hence the latter is a character.

Now, remember that for all $g \in G$, the complex number $\lambda(g)$ is a root of unity. Therefore $\lambda(g)\overline{\lambda(g)} = 1$. So we have,

$$\begin{aligned}\langle \chi\lambda, \chi\lambda \rangle &= \frac{1}{|G|}\sum_{g\in G} \chi(g)\lambda(g)\overline{\chi(g)\lambda(g)} \\ &= \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\chi(g)} \\ &= \langle \chi, \chi \rangle.\end{aligned}$$

But χ is irreducible iff $\langle \chi, \chi \rangle = 1$, therefore $\chi\lambda$ is irreducible iff χ is irreducible. □

So, finding linear characters can help us find new characters. We shall soon discuss how this can be done, but first we need to describe a way of getting a character of G from a character of G/N where N is normal.

HW See how easier it now is to find the complete character table of S_4.

17.2 Lifted characters

If we know that G has a normal subgroup N then we know that G/N is also a group. But since G/N is smaller than G we might already know its characters. Therefore it would be useful if we had a method of going from a character of G/N to one of G.

Theorem 17.2 *Let $N \lhd G$ and and let $\tilde{\chi}$ be a character of G/N. Define $\chi : G \to \mathbb{C}$ by*

$$\chi(g) = \tilde{\chi}(Ng).$$

Then the function χ is a character of G and χ and $\tilde{\chi}$ have the same degree (dimension).

Note the natural way in which χ was defined based on $\tilde{\chi}$: to calculate $\chi(g)$ find the coset of N in which g lies and let $\chi(g)$ be the value of $\tilde{\chi}$ on that coset. This character is called the *lift* of $\tilde{\chi}$ to G.

The next theorem tells us that if we know the character table of G/N then we can write down as many irreducible characters of G as there are of G/N.

But first recall that we have defined the kernel of a character χ as

$$\ker \chi = \{g \in G : \chi(g) = \chi(1) = n\},$$

and that by Theorem 11.4, $\ker \chi$ is a normal subgroup of G.

Theorem 17.3 (Theorem 17.3 in [JL] *.] Let $N \lhd G$. Associate with each character of G/N with its lift to G. This gives a bijective correspondence between the set of characters of G/N and the set of characters χ of G which have the property that $N \leq \ker \chi$.*

Under this correspondence, irreducible characters of G/N correspond to irreducible characters of G which have N in their kernel.

Example 17.1 *This is Example 17.4 in [JL]. Let $G = S_3$, and let*

$$N = \{id, (12)(34), (13)(24), (14)(23)\}.$$

Then it is easy to see that $N \lhd G$.

Let a be the coset $N(123)$ and let b be the coset $N(12)$. Then

$$G/N = \langle a, b : a^3 = b^2 = N = 1, ab = a^{-1}b\langle.$$

Therefore G/N is isomorphic to D_3 or S_3. But we already have the character table of S_3¿ Therefore the character table of G/N is:

g	N	$N(12)$	$N(123)$
$\chi_1(g)$	1	1	1
$\chi_2(g)$	1	-1	1
$\chi_3(g)$	2	0	-1

We can now calculate lifts to give us the following three irreducible characters of S_4. Note that $\chi((12)(34)) = \tilde{\chi}(N)$ and $\chi((1234)) = \tilde{\chi}(N(13))$.

g	id	(12)	(123)	$(12)(34)$	(1234)
$\chi_1(g)$	1	1	1	1	1
$\chi_2(g)$	1	-1	1	1	-1
$\chi_3(g)$	2	0	-1	2	0

17.3 Finding all linear characters

Now, in our study of groups we have already seen one very important normal subgroup of any group, that is, the centre $Z(G)$ (the centre could, of course, be trivial, that is, equal to $\{1\}$ or G itself). We now define another very important normal subgroup of G which is also related to the commutativity (or lack of it) of G. In the context of our discussion, this normal subgroup is important because it will allow us, in principle, to determine all the linear characters of G.

Firstly, let g and h be two elements of G. The *commutator* of g, h, written $[g, h]$ is defined to be the product

$$g^{-1}h^{-1}gh.$$

Note that the commutator seems to be trying to capture whether or not g and h commute, for $[g, h] = 1$ iff g and h commute. Now, collect all commutators for all pairs of elements and construct all possible products of these elements. The resulting group is called the *derived subgroup* of G and is denoted by G'. Therefore G' is the subgroup of G generated by all commutators, or

$$G' = \langle [g, h] : g, h \in G \rangle.$$

It is easy to show that $G' = \{1\}$ iff G is abelian and also that G' is a normal subgroup of G.

It is not always easy to determine G', although the examples you will be meeting will not be too difficult. Here is an easy example.

Example 17.2 *This is example 17.8 in [JL]. Let $G = S_3$. Clearly $[g, h]$ is always an even permutation (Why?). So $G' \leq A_3$. Also, if $g = (12)$ and $h = (23)$ then $[g, h] = (123)$. But (123) generates the whole of A_3, therefore $G' = A_3$.*

Theorems 17.9 and 17.10 of [JL] are not difficult group theoretic properties of G'. We have already mentioned two: G is abelian iff $G' = \{1\}$ and $G' \lhd G$. Other important results are: (i) if *chi* is a linear character then $G' \leq \ker \chi$ (Prop 17.9) — this is very easy because multiplication of linear characters is simply multiplication in $\mathbb{C}$ which is commutative; (ii) G/G' is always abelian (Prop 17.10) – this is a not difficult technical result using only group theory without any representations. But for our purpose the interest is in the following which follows from these properties of G' and the earlier results on lifts. We shall concentrate on the use of this result to obtain irreducible characters of G.

Theorem 17.4 (Theorem 10.10 in [JL] *.] The linear characters of G are precisely the lift to G of the irreducible characters of G/G'. In particular, the number of distinct linear characters of G is equal to $|G|/|G'|$ and so divides $|G|$.*

Therefore to use this theorem to find all the linear characters of G we need to be able to (i) find G'; (ii) find G/G' (which is always abelian and therefore has all characters linear); (iii) find the characters of this smaller group G/G';

and (iv) lift the characters of G/G' to G. This might not always be easy but you will meet examples for which carrying out this formula is not too difficult. And sometimes this result is no help at all. If G is abelian, $G' = \{1\}$ and G/G' is simply G itself! It could also be that G has few linear characters so that finding them all is still a l,ong way away from finding the complete character table, as we see in this example.

Example 17.3 *This is Examples 17.12 and 17.13 in [JL]. We shall find all the linear characters of S_n. Example 17.12 first determines S_n for all $n \geq 4$. It is clear that every $[g,h]$ is an even permutation (why?) so $S'_n \leq A_n$ (no need for Proposition 17.10(2)). Then, if $p, q, r \in \{1, 2, \ldots, n\}$, and if the permutations g and h are $(p\ q)$ and $(q\ r)$, respectively, then their commutator $[g,h]$ is equal to the cycle $(p\ q\ r)$. Therefore every 3-cycle is in S'_n. But it is well-know that the 3-cycles generate A_n, therefore $A_n \leq S'_n$. So, $S'_n = A_n$.*

Then Example 17.13 uses this to find the linear characters of S_n. We have that $S_n/S'_n = S_n/A_n = \{A_n, A_n(1\ 2) \simeq C_2$. But C_2 has only two characters, the trivial character $\overline{\chi}_1$ and the character $\overline{\chi}_2$ which takes the value on on the identity and the value -1 on the other element. Lifting these two characters to S_n give us the trivial character and the sign character.

So this method does not give us any new linear character of S_n—we already knew about them. But what it tells us is that these are the only *linear characters of S_n, therefore it is useless to try and find any others.*

17.4 Finding normal subgroups

Once we have found the character table we can use it to determine various properties of G, the easiest of which is to determine whether G is simple.

Recall first that the kernel of a character χ, which is a normal subgroup of G, is easily located from the character table. Just go through the row corresponding to χ and collect all those elements g such that $\chi(g) = 1$. It is true, of course, that any intersection of kernels of characters is a normal subgroup of G. The remarkable fact is that *every* normal subgroup of G arises this way.

Theorem 17.5 (Proposition 17.5 in [JL]) *.] If $N \lhd G$ then there exist irreducible characters $\chi_1, \ldots, \chi_s$ of G such that*

$$N = \cap_{i=1}^{s} \ker \chi_i.$$

This result makes it possible to tell easily from the character table of G whether or not G is simple.

Theorem 17.6 (Proposition 17.6 in [JL) *.] The group G is not simple iff*

$$\chi(g) = \chi(1)$$

for some non-trivial irreducible character of G, and some non-identity element g of G.

HW.

1. Chapter 17 of [JL], Exercises 1, 4, 5, 7.
2. Read Chapter 18, Sections 1 and 2.
3. Chapter 18 Exercises 1 and 2.

18 An application: The spectrum of a graph

In the sequel, Γ will be a simple graph on the vertex-set $V = \{1, 2, \ldots, n\}$ and $A = A(\Gamma)$ will be the *adjacency matrix* of Γ, that is, $A_{ij} = 1$ if i, j are adjacent in Γ and $A_{ij} = 0$ otherwise. An *automorphism* of Γ is a permutation p of V such that i, j are adjacent iff $p(i), p(j)$ are adjacent. The group of all automorphisms of Γ is denoted by $\mathrm{Aut}(\Gamma)$. Let p be any permutation of V. Let A^p be the matrix whose ij entry is $A_{p(i)p(j)}$. Then it is clear that p is an automorphism of Γ iff $A = A^p$. (If you need convincing, draw a small graph, write down its adjacency matrix, and test with an automorphism p.)

Let the matrix $P = P(p)$ be the permutation matrix corresponding to p, that is, $P_{ij} = 1$ if $p(i) = j$, $P_{ij} = 0$ otherwise. Note that $P^{-1} = P(p^{-1})$. The matrices P give a linear representation of $\mathrm{Aut}(\Gamma)$, and this representation will often determine what types of eigenvectors and eigenvalues the adjacency matrix can have. The link between the matrix A and this representation of $\mathrm{Aut}(\Gamma)$ is given by the following theorem.

Theorem 18.1 *Let P be the permutation matrix corresponding to the permutation p of V, and let A be the adjacency matrix of Γ. Then p is an automorphism of Γ iff $AP = PA$.*

Proof. To be able to concentrate on one edge at a time we define $D(ij)$ to be the matrix all of whose entries are 0 except the ij-entry which is 1. Then, of course,

$$A = \sum_{ij \in E(\Gamma)} D(ij).$$

Consider $P^{-1}AP$. We need to show that this product equals A iff p is an automorphism of Γ.

Suppose $p(i) = k$ and $p(j) = l$. Since $p^{-1}(k) = i$, there is only one non-zero entry in the column i of P^{-1}, namely in row k. Therefore $P^{-1}D(ij) = D(kj)$. Similarly, $D(kj)P = D(kl)$. Therefore

$$P^{-1}D(ij)P = D(kl) = D(p(i)p(j)).$$

Therefore

$$\begin{aligned} P^{-1}AP &= P^{-1}\Big(\sum_{ij\in E(\Gamma)} D(ij)\Big)P \\ &= \sum_{ij\in E(\Gamma)} P^{-1}D(ij)P \\ &= \sum_{ij\in E(\Gamma)} D(p(i)p(j)) \\ &= A^p. \end{aligned}$$

But we have already observed that $A^p = A$ iff p is an automorphism of Γ. □

From now on, out treatment will be based on Cvetkovic, Doob and Sachs, *Spectra of Graphs* [CDS]. Suppose P is the representation of $G = \mathrm{Aut}(\Gamma)$ as permutation matrices, that is, for every $p \in G$ there is the matrix $P(p)$ defined as above. Then A, the adjacency matrix of Γ, commutes with every $P(p)$.

18.1 The number of distinct eigenvalues of A

Since A is symmetric, there exists T such that

$$T^{-1}AT = D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$$

where the eigenvalues λ_i are arranged such that $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$. Suppose there are $t \leq n$ distinct eigenvalues and $D_1, \ldots, D_t$ are the submatrices of D corresponding to the t blocks of equal eigenvalues. Therefore

$$D = D_1 \oplus \ldots \oplus D_t,$$

where each D_i is a diagonal matrix with all its entries equal. Let us apply T to A and the matrices $P(p)$. Let

$$T^{-1}P(p)T = Q(p).$$

Then D commutes with every $Q(p)$ (since $AP = PA$, $(T^{-1}AT)(T^{-1}PT) = (T^{-1}PT)(T^{-1}AT)$). But then, $Q(p)$ has to decompose into t blocks corresponding to the eigenvalues multiplicities. (This is an elementary matrix algebra result, not requiring any of the theory we have developed in this course. For example, check that if

$$\left(\begin{array}{cc|cc} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{array}\right) \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) \left(\begin{array}{cc|cc} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{array}\right)$$

then $B = C = 0$.)

So we can write

$$Q(p) = Q_1(p) \oplus \ldots \oplus Q_t(p)$$

where each Q_i is a square matrix whose size is equal to the multiplicity of the i-th distinct eigenvalue of A. Now, apply Maschke's Theorem to each of the Q_i separately to get matrices S_i such that $S_i^{-1}Q_iS_i$ decomposes into m_i irreducibles (counting multiplicities). Note that $S_i^{-1}D_iS_i = D_i$, therefore the matrix

$$S = S_1 \oplus \ldots \oplus S_t$$

reduces Q to its irreducible constituents and leaves D unchanged. The number of irreducibles of Q is $m = \sum_{i=1}^{t} m_i$ and clearly $m \geq t$. We have therefore proved the following.

Theorem 18.2 *Let Γ be a graph and let $G = Aut(\Gamma)$ and also let A be the adjacency matrix of Γ. Let P be the permutation matrix representation of G. Suppose that A has t distinct eigenvalues and suppose that the decomposition of P into irreducibles has m irreducibles, counting multiplicities. Then $t \leq m$.*

Example 18.1 *Let Γ be the graph shown in Figure 18.1. Then $G = Aut(\Gamma) \simeq S_3 \simeq D_3$. The character table of G is therefore given by*

g	1	$\{a, a^2\}$	$\{b, ab, a^2b\}$
$\chi_1(g)$	1	1	1
$\chi_2(g)$	1	1	-1
$\chi_3(g)$	2	-1	0

where a and a^2 correspond to the two rotations about the central vertex, and b, ab, a^b correspond to the permutations which interchange two of the three "wings" of the "windmill", leaving the other fixed.

The defining character π of the representation P of G is given by

g	1	$\{a, a^2\}$	$\{b, ab, a^2, b\}$
$\pi(g)$	13	1	5

.

Let $\pi = \alpha\chi_1 + \beta\chi_2 + \gamma\chi_3$. We find α, β, γ in the usual fashion, giving that $\alpha = 5, \beta = 0, \gamma = 4$. Therefore the number of irreducible components of P is $5 + 4 = 9$ and we deduce, without even looking at the adjacency matrix of Γ, that it can have at most nine distinct eigenvalues. In fact, if it has this number of distinct eigenvalues, then this would mean, from $\pi = 5\chi_1 + 4\chi_3$ and the fact that $\dim(\chi_1) = 1$ and $\dim(\chi_3) = 2$, that it would have five distinct simple eigenvalues and four distinct eigenvalues with multiplicity 2; and $5.1 + 4.2 = 13$ which checks out to the total number of eigenvalues (counting multiplicities) of Γ.

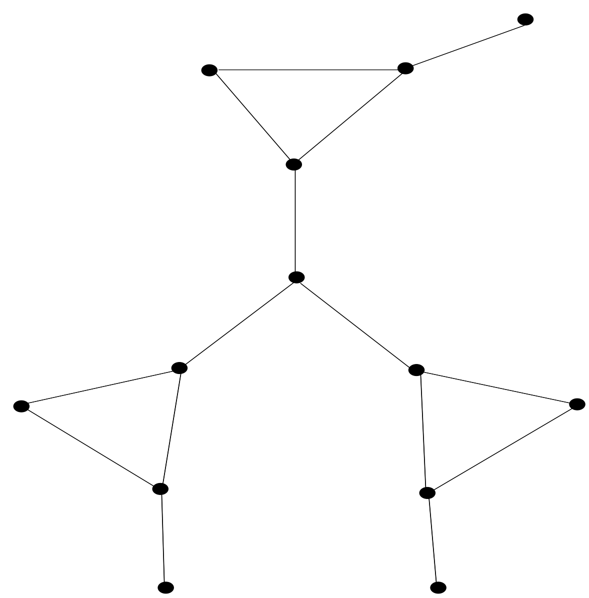

Figure 1: How many distinct eigenvalues does this graph have?

HW: Show, without using its adjacency matrix, that the graph in Figure 18.1 can have at most four distinct eigenvalues.

18.1.1 The simple eigenvalues

The above is only a sample of what can be deduced about the distinct eigenvalues of a graph from knowledge of its automorphism group. In the rest of

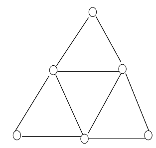

Figure 2: *This graph can have at most four distinct eigenvalues*

this subsection we present some more such results which might help to bring the above into better context. None of the sequel in this subsection uses group representations.

Lemma 18.1 *Let P be the matrix corresponding to an automorphism p of the graph Γ. If x is an eigenvector of of A corresponding to the eigenvalue λ, then Px is also an eigenvector of A corresponding to the eigenvalue λ.*

Proof. $Ax = \lambda x$. But $APx = PAx = P(\lambda x) = \lambda Px$. □

Theorem 18.3 *Let λ be a simple eigenvalue of A and let x be a corresponding eigenvector with real components. If P is a matrix corresponding to an automorphism of Γ, then $Px = \pm x$,*

Proof. Because λ is simple and x and Px are both eigenvectors corresponding to λ, these vectors are linearly dependent. That is, $Px = kx$ for some $k \in \mathbb{R}$. But because P is a permutation matrix, $P^s = I$ for some $s \in \mathbb{N}$. Therefore $k = \sqrt[s]{1} = \pm 1$. □

Theorem 18.4 *Suppose all the eigenvalues of Γ are simple. Then every non-trivial automorphism of Γ has order 2. This, in particular, implies that $Aut(\Gamma)$ is abelian.*

Proof. Let P be any permutation matrix corresponding to an automorphism of Γ, and let $\{x_1, \ldots, x_n\}$ be a complete set of eigenvectors of Γ. Because $Px_i = \pm x_i$ for each i, $P^2 x_i = x_i$. But the x_i form a basis for $\mathbb{R}^n$, therefore $P^2 = I$, the identity. □

Example 18.2 *Since the permutation* (1 4 2 3)(5 6) *is an automorphism of the graph shown in Figure 18.2 and this permutation has order 4, we can deduce, without looking at the graph's adjacency matrix, that it cannot have all its eigenvalues simple.*

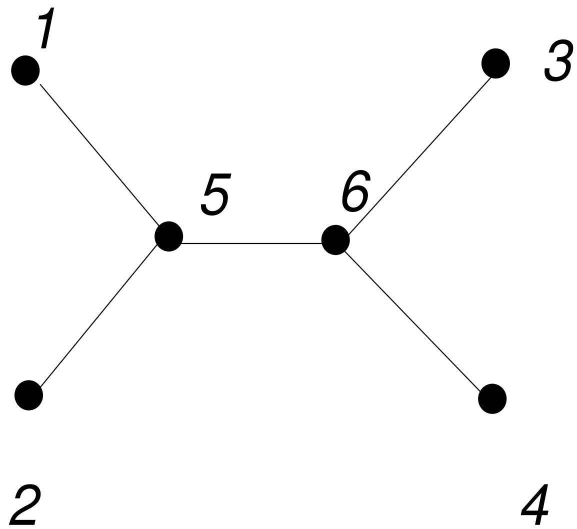

Figure 3: Are all the eigenvalues simple?

18.2 Finding the eigenvalues

Sometimes, one can exploit the symmetries of a graph in order to simplify the problem of finding its eigenvalues. For example, one might be able to reduce the problem of finding the eigenvalues of a graph on twenty vertices to five 4×4 problems rather than one 20×20 problem. The technique which we are going to describe to do this is often used molecular chemistry.

What we shall do is essentially the reverse of what we did in the previous section. There we applied the matrix which diagonalised A to P and then decomposed P into irreducibles. Here, we shall apply to A the matrix which decomposes P into irreducibles, and then apply Schur's Lemma.

First we need an extension of Schur's Lemma. Remember that Schur's Lemma talked about matrices which commute with a representation — which is just what we have here with the matrix A and the representation P — but the representation needed to be irreducible. What if P is reducible, as is generally the case with the permutation representation of the automorphism group of a graph?

Consider first a simple example. Suppose X is a reducible matrix representation of a group G, and suppose

$$X = X_1 \oplus X_2$$

where X_1, X_2 are *non-equivalent* irreps. Suppose the matrix

$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

commutes with X, and that A and D have the same sizes as X_1 and X_2, respectively. Then we get that $X_1 B = B X_2$ and $X_2 C = C X_1$. But X_1 and X_2 are irreducible and non-equivalent. Therefore, by Schur's Lemma, $B = C = 0$. This result can be extended to give that, if

$$X = m_1 X_1 \oplus \ldots \oplus m_t X_t$$

where the X_i are non-equivalent irreps, and if K commutes with all the $X(g)$, then K must decompose into blocks

$$K = K_1 \oplus \ldots \oplus K_t$$

where the size of K_i is $(m_i \dim(X_i)) \times (m_i \dim(X_i))$.

Now, let Γ, G, A, P be as in the previous section. By Maschke's Theorem, there is a matrix U such that

$$U^{-1} P(p) U = m_1 P_1 \oplus \ldots \oplus m_t P_t(p),$$

where the P_i are irreps and non-equivalent. We now apply U to A to give

$$B = U^{-1} A U.$$

The eigenvalues of B are the same as those of A. Also, B commutes with $U^{-1} P U$. Therefore B has the block structure described above. And the eigenvalues of B are precisely the eigenvalues of these smaller blocks.

Each block corresponds to that submodule S_{χ_i} of $\mathbb{R}^n$ which can be described as follows: each S_{χ_i} consists of the sum of all of the irreducible submodules of the representation P which have character χ_i. If we can find these subspaces of $\mathbb{R}^n$ we can then solve the eigenvalue problem for each of these smaller subspaces — effectively this means finding the eigenvalues for the smaller matrix B_i.

How do we find this smaller subspace? We need a theorem form [JL] whose proof we do not give.

Theorem 18.5 (Theorem 14.26 in [JL) *] If χ is an irreducible character of G and V is any $\mathbb{C}G$-module, then the sum of those $\mathbb{C}G$-submodules of V which have character χ is equal to Vr where*

$$r = \sum_{g \in G} \chi(g^{-1}) g.$$

Note that r is an alement of $\mathbb{C}G$, and we are using again the fact that $\mathbb{C}G$ acts on V as an extension of the action of G on V.

So what we do to find the eigenvalues of A is the following.

1. Take a basis $\{e_1, \ldots, e_n\}$ for $\mathbb{R}^n$, say the standard basis.
2. Find the irreducible characters of the permutation representation of $\mathrm{Aut}(\Gamma)$ using the character table of $G = \mathrm{Aut}(\Gamma)$.
3. For each such character χ calculate the matrix $R = \sum_{p \in \mathrm{Aut}(\Gamma)} \chi(p^{-1}) P(p)$ and let $v_i = Re_i$.
4. Then the vectors $\{v_1, \ldots, v_n\}$, which in general are not linearly independent, span the submodule S_χ of $\mathbb{R}^n$ which is the sum of all the irreducible submodules of P which have character χ.
5. Solve the eigenvalue problem for A on the space S_χ which has dimension smaller than n.
6. Repeat for all the irreducible characters of P.

We shall illustrate this method with an example taken from [CDS].

Example 18.3 *Let Γ be the path P_3 shown in Figure 18.3. Of course, we do not need any special methods to find the eigenvalues of such a small graph, but we shall use it as an illustration.*

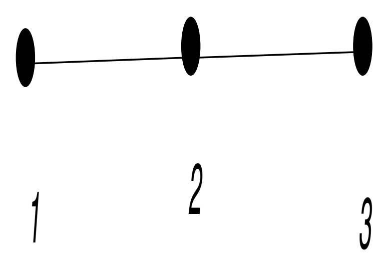

Figure 4: The path P_3

The adjacency matrix of Γ is

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The automorphism group of Γ *is* $G = \{id, (1\ 3)(2)\} = \{1, a\}$. *Let* χ *be the character of the permutation representation of* G. *The character table of* G *and the character* χ *are given below.*

	1	a
χ_1	1	1
χ_2	1	-1
χ	3	1

As usual, we find that

$$\chi = 2\chi_1 + \chi_2.$$

We can now reduce finding the eigenvalues of A *to two smaller problems corresponding to the characters* χ_1 *and* χ_2.

Eigenvectors and eigenvalues from χ_1

Let the matrix representation of $Aut(\Gamma)$ *be*

$$P(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$P(a) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Let $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ *and* $e_3 = (0, 0, 1)$. *Therefore*

$$\begin{aligned} R &= \chi_1(1^{-1})P(1) + \chi_1(a^{-1})P(a) \\ &= 1.\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + 1.\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Therefore

$$v_1 = Re_1 = e_1 + e_3,$$

and

$$v_2 = Re_2 = 2e_2$$

and

$$v_3 = Re_3 = e_1 + e_3.$$

Therefore v_1, v_2, v_3 *span the two-dimensional subspace of* $\mathbb{R}^3$ *given by*

$$\{(\alpha,\beta,\alpha) : \alpha,\beta \in \mathbb{R}\},$$

and this is the eigenspace required. Therefore we solve the eigenvalue problem for A for this smaller subspace:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \alpha \end{pmatrix} = \lambda \begin{pmatrix} \alpha \\ \beta \\ \alpha \end{pmatrix}$$

giving us

$$\begin{pmatrix} \lambda & -1 \\ 2 & -l\lambda \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

with the solution $\lambda = \pm\sqrt{2}$.

Eigenvectors and eigenvalues from χ_2

We work with the matrix representation of $Aut(\Gamma)$ *as above, and with the same* $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ *and* $e_3 = (0,0,1)$. *Now, let*

$$\begin{aligned} R &= \chi_2(1^{-1})P(1) + \chi_2(a^{-1})P(a) \\ &= 1. \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + (-1). \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Therefore

$$v_1 = Re_1 = e_1 - e_3,$$

and

$$v_2 = Re_2 = 0$$

and

$$v_3 = Re_3 = e_3 - e_1.$$

Therefore v_1, v_2, v_3 *span the one-dimensional subspace of* $\mathbb{R}^3$ *given by*

$$\{(\alpha, 0, -\alpha) : \alpha \in \mathbb{R}\},$$

and this is the eigenspace required. Therefore we solve the eigenvalue problem for A for this smaller subspace:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ -\alpha \end{pmatrix} = \lambda \begin{pmatrix} \alpha \\ 0 \\ -\alpha \end{pmatrix}$$

giving immediately the solution $\lambda = 0$.

HW: Find, using the above method, the eigenvalues of the graph $K_{1,3}$.

18.2.1 Cayley graphs of abelian groups

When the group G is abelian and the graph Γ has a structure closely related to the group, it can become very easy to determine the eigenvalues and eigenvectors of Γ from the character table of G. In order to illustrate the connection between the characters of G and the eigenvalues of Γ we shall give one result but without a proof. First we need to define what we mean by a Cayley graph. Let G be a group and let $S \subseteq G$ be a subset of G which generates G, which has the property that if $s \in S$ then $s^{-1} \in S$, and which does not contain 1. The *Cayley graph* $\Gamma = \mathrm{Cay}(G, S)$ is defined as follows. The vertex set of Γ is G, that is, the vertices of G are the elements of G. Then, a vertex $g \in G$ is made adjacent to all the vertices gs for all $s \in S$. We leave it as an exercies to show that:

1. Since $1 \notin S$, Γ has no loops;
2. Since $s \in S \rightarrow s^{-1} \in S$, the edges of Γ are not directed, that is, if g is adjacent to h then h is adjacent to g;
3. Since S generates G, Γ is connected.

We can now state this theorem.

Theorem 18.6 *Let $\Gamma = Cay(G, S)$ be a Cayley graph of an abelian group G. Then the rows of the character table of G are a complete set of eigenvectors of the adjacency matrix A of Γ. That is, for each character, the n-tuple of values of character on the elements of G form an eigenvector of A. The eigenvector corresponding to the the character χ is given by*

$$\sum_{s \in S} \chi(s).$$

HW:

1. Without using its adjacency matrix, find the eigenvalues of C_n, the cycle on n vertices.
2. Show that the graph in Figure 2 is a Cayley graph of an abelian group. Hence find its eigenvalues without using its adjacency matrix.

19 Conclusion: What next?

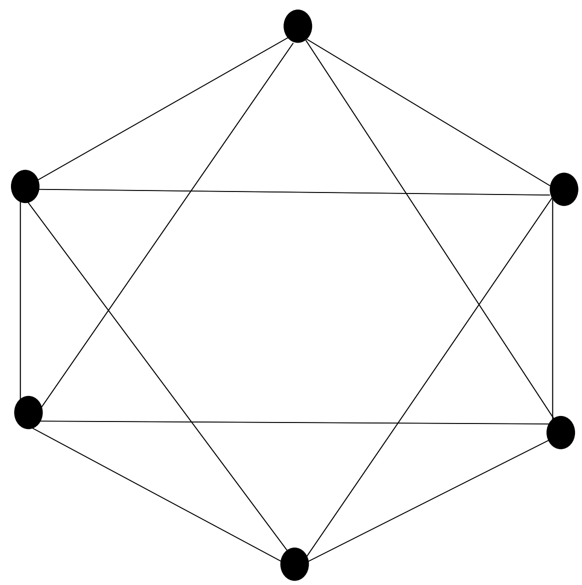

Figure 5: A Cayley graph of an abelian group