Maths 721 Notes

2020

Contents

1 Lecture 1

In the first half of this course we will cover three main topics:

- representations;
- modules;
- characters.

We will further see that representations and modules are essentially the same, and that modules and characters are essentially the same; and hence all three are essentially the same.

From now on G is a group.

1.1 Representations

Definition 1.1. A **representation** of a group G over a field F is a group homomorphism from G to $\mathrm{GL}(n, F)$, where n is the **degree** of the representation.

Explicitly, a representation is a function $\rho : G \to \mathrm{GL}(n, F)$ such that for all $g, h \in G$;

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

(ii) $1_G\rho = I_n$,

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

Note the use of the (incredibly shit) postfix function notation.

Example 1.2. Take D_4, the Dihedral group of order 8. It has the following group presentations

$$\begin{aligned} D_4 &= \langle a, b \mid a^4 = 1, b^2 = 1, a^b = a^{-1} \rangle \\ &\cong \langle (1\ 2\ 3\ 4), (1\ 4)(2\ 3) \rangle, \end{aligned}$$

where $a^b = bab^{-1}$ is conjugation of a by b. By defining the matrix subgroup

$$H = \left\langle A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle$$

and defining $\rho : D_4 \to \mathrm{GL}(n, F)$ where $F = \mathbb{R}, \mathbb{C}$, by $a \mapsto A$ and $b \mapsto B$, and $a^i b^j \mapsto A^i B^j$ for $0 \le i \le 3$, and $0 \le j \le 1$. Hence we have ρ is a representation of D_4 over F. ◀

Example 1.3. Take $\mathbb{Q}_8$ the Quaternion group of order 8, which has the following group presentations

$$\begin{aligned} \mathbb{Q}_8 &= \langle a, b \mid a^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle \\ &\cong \langle \bar{a} = (1\ 6\ 2\ 5)(3\ 8\ 4\ 7), \bar{b} = (1\ 4\ 2\ 3)(5\ 7\ 6\ 8) \rangle \end{aligned}$$

Define
$$H = \left\langle A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle \subset \mathrm{GL}(2, \mathbb{C}).$$
Then $\rho : \mathbb{Q}_8 \to \mathrm{GL}(2, \mathbb{C})$ defined by $a^k b^\ell \mapsto A^k B^\ell$ is a group representation of $\mathbb{Q}_8$ over $\mathbb{C}$ of degree 2. ◀

Definition 1.4. Let G be a group and define
$$\begin{aligned} \rho : G &\to \mathrm{GL}(n, F) \\ g\rho &= I_n \end{aligned}$$
for all $g \in G$. Then ρ is a representation, called the **trivial representation** of arbitrary of degree.

It follows from the trivial representation that any group G has a representation of an arbitrary degree.

Let $\rho : G \to \mathrm{GL}(n, F)$ be a group homomorphism, and take $T \in \mathrm{GL}(n, F)$. Then
$$(T^{-1}AT)(T^{-1}BT) = T^{-1}(AB)T.$$
Thus, given ρ define σ such that
$$g\sigma = T^{-1}(g\rho)T$$
for all $g \in G$. As for all $g, h \in G$, one has
$$\begin{aligned} (gh)\sigma &= T^{-1}\big((gh)\rho\big)T \\ &= T^{-1}(g\rho)(h\rho)T \\ &= T^{-1}(g\rho)TT^{-1}(h\rho)T \\ &= (g\sigma)(h\sigma), \end{aligned}$$
and so σ is a group homomorphism; and hence a representation.

Definition 1.5. Define
$$\rho : G \to \mathrm{GL}(m, F), \qquad \sigma : G \to \mathrm{GL}(n, F)$$
to both be representation of G over F. We say that ρ **is equivalent to** σ if $n = m$ and there exists $T \in \mathrm{GL}(n, F)$ such that $g\sigma = T^{-1}(g\rho)T$.

Proposition 1.6. *Equivalence of representations is an equivalence relation.*

Proof. Reflexivity is clear by taking $T = I_n$. For symmetry, take T to be its inverse. For transitivity, if
$$g\sigma = T^{-1}(g\rho)T, \qquad g\rho = S^{-1}(g\eta)S,$$
then
$$g\sigma = (ST)^{-1}(g\eta)(ST).$$
□

Definition 1.7. Define the **kernel** of the representation $\rho : G \to \mathrm{GL}(n, F)$ as $\ker\rho = \{g \in G \mid g\rho = I_n\}$.

Proposition 1.8. *The kernel of a representation of G is a normal subgroup of G; i.e.* $\ker\rho \lhd G$.

Proof. Suppose $g \in \ker\rho$ and $h \in G$ is arbitrary. Then

$$(hgh^{-1})\rho = (h\rho)(g\rho)(h^{-1}\rho) = (h\rho)I_n(h\rho)^{-1} = (h\rho)(h\rho)^{-1} = I_n,$$

and so $hgh^{-1} \in \ker\rho$. As $\ker\rho$ is closed under conjugation, it is a normal subgroup of G. □

Definition 1.9. We say ρ is a **faithful** representation of G if $\ker\rho = \{1_G\}$.

Example 1.10. For the trivial representation $\rho : G \to \mathrm{GL}(n, F)$ with $g \mapsto I_n$ for all $g \in G$, we have $\ker\rho = G$. Hence the representation is not faithful. ◀

Lemma 1.11. *Suppose G is a finite group, and ρ is a representation of G over F. Then ρ is faithful if, and only if,* $\operatorname{im}\rho \cong G$.

Proof. Immediate from the first isomorphism theorem. □

1.2 FG-Modules

Suppose G is a group, and $F = \mathbb{R}, \mathbb{C}$. Given $\rho : G \to \mathrm{GL}(n, F)$, with $V = F^n$, let $v = (\lambda_1, \ldots, \lambda_n) \in V$ for $\lambda_i \in F$ be a row vector. Moreover, note that $g\rho$ is an $n \times n$ matrix for all $g \in G$. Thus, we have $v \cdot (g\rho) \in V$, and satisfies the following properties:

(i) $v \cdot \big((gh)\rho\big) = v \cdot (g\rho)(h\rho)$;

(ii) $v \cdot (1_G\rho) = v$;

(iii) $(\lambda v) \cdot (g\rho) = \lambda\big(v \cdot (g\rho)\big)$;

(iv) $(u + v) \cdot (g\rho) = u \cdot (g\rho) + v \cdot (g\rho)$.

We often will omitted the $\cdot$ in the operation, and write $v(a\rho)$ for $v \cdot (a\rho)$.

Example 1.12. Recall D_4 and its given presentation from a previous example. We have

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

If $v = (\lambda_1, \lambda_2)$, then we have

$$v(a\rho) = (-\lambda_2, \lambda_1), \qquad v(b\rho) = (\lambda_1, -\lambda_2).$$

◀

Definition 1.13. Let V a vector space over the field $F = \mathbb{R}, \mathbb{C}$, and let G be a group. We say V is a FG**-module** if a multiplication $v \cdot g$ for $v \in V$, and $g \in G$ is defined such that:

(i) $v \cdot g \in V$;

(ii) $v \cdot (gh) = (v \cdot g) \cdot h$;

(iii) $v \cdot 1_G = v$;

(iv) $(\lambda v) \cdot g = \lambda(v \cdot g)$;

(v) $(u + v) \cdot g = u \cdot g + v \cdot g$.

This generalises the previous discussion from a matrix group to an arbitrary group.

Note that properties (i), (iv), and (v) imply that the map $v \mapsto v \cdot g$ is an endomorphism of V (a linear map from V to itself).

Definition 1.14. Suppose V is an FG-module and B is a basis for V. For $g \in G$, let $[g]_B$ denote the matrix of the endomorphism $v \mapsto v \cdot g$ of V relative to the basis B.

2 Lecture 2

Theorem 2.1. *Let $\rho : G \to GL(n, F)$ be a representation of G over F.*

(I) *If $V = F^n$ is an FG module and G acts on V by $v \cdot g = v(g\rho)$ there exists a basis B of V such that $g\rho = [g]_B$.*

(II) *The map $g \mapsto [g]_B$ is a representation for G over F.*

Proof. Choose the standard basis $B = [e_1, \ldots, e_n]$.

Since V is an FG-module we have $v(gh) = (vg)h$ for all $g, h \in G$ and $v \in V$. Thus $[gh]_B = [g]_B[h]_B$ so the map is a homomorphism. We now check that $[g]_B$ is invertable for all $g \in G$. We know $v \cdot 1_G = (vg)g^{-1}$ so $I_n = [g]_B[g^{-1}]_B$ and thus $[g]_B$ has an inverse. □

Example 2.2. Recall the representation of $G = D_4$ from a previous example. Define an FG-module $V = F^2$ with the action defined by taking vg to $v(g\rho)$.

$$\begin{aligned} v_1 &= (1, 0), \quad v_1 a = v_2, \quad v_1 b = v_1, \\ v_2 &= (0, 1), \quad v_1 a = -v_1, \quad v_1 b = -v_2. \end{aligned}$$

In this basis we recover our representation

$$a \mapsto [a]_B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad b \mapsto [b]_B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

◀

We now provide an equivalent basis-dependent definition for an FG-module.

Lemma 2.3. *Let V a vector space over the field $F = \mathbb{R}, \mathbb{C}$ with basis $B = [v_1, \ldots, v_n]$, and let G be a group. If a multiplication $v \cdot g$ for $v \in B$, and $g \in G$ is defined such that:*

(i) $v \cdot g \in V$;

(ii) $v \cdot (gh) = (v \cdot g) \cdot h$;

(iii) $v \cdot 1_G = v$;

(iv) $(\sum_{i=1}^n \lambda_i v_i) \cdot g = \sum_{i=1}^n \lambda_i (v_i \cdot g)$ *for all* $\lambda_i \in F$;

then V is an FG-module.

Definition 2.4. The trivial module of a group over F is a one dimensional vector space V over F such that $vg = v$ for all $v \in V$ and $g \in G$.

Definition 2.5. An FG-module is faithful if 1_G is the only $g \in G$ such that $vg = v$ for all $v \in V$.

Theorem 2.6. *Let V be an FG-module with basis B and ρ a representation of group G over F defined by taking $g \mapsto [g]_B$.*

(i) If B' is another basis of V then the map $g \mapsto [g]_{B'}$ is a representation of G equivalent to ρ.

(ii) If representation σ is equivalent to ρ then there exists basis B'' such that $\sigma(g) = [g]_{B''}$ for all $g \in G$.

Proof. Taking T to be the change of basis matrices, the two representations are equivalent. $\square$

Example 2.7. Let $G = C_3 = \langle a \mid a^3 = 1 \rangle$ and representation $\rho : G \to GL(n, F)$ defined by

$$a \mapsto \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

We attempt to construct an FG-module with group action described by ρ. Take $V = F^2$ with basis $B = [v_1, v_2]$. Define the action of G on V by

$$v_1 a = v_2, \quad v_2 a = -v_1 - v_2.$$

Let us now choose alternate basis $B' = [u_1 = v_1, u_2 = v_1 + v_2]$. The action of G on this basis is described by

$$u_1 a = -u_1 + u_2, \quad u_2 a = -u_1.$$

This gives us a representation

$$a \mapsto [a]_{B'} = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}.$$

To verify this construction we write our change of basis matrix as

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

and verify that

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

◀

Definition 2.8. The permutation module of a group $G \leq S_n$ is an n-dimensional vector space V with basis $B = [v_1, \ldots, v_n]$ and action by G defined by

$$v_i g = v_{ig}$$

for all $g \in G$ where ig is the image of i under $g \in S_n$.

It follows from Caley's theorem that every group has a faithful FG-module.

Example 2.9. Take $G = S_4$ and pick $g = (1\ 2)$ and $h = (1\ 2\ 3\ 4)$. We have representations

$$[g]_B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad [h]_B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

◀

2.1 Module Reducibility

Definition 2.10. Let V be an FG-module. We call W a submodule of V if W is a vector subspace of V and W is closed under the action of G. We then write $W < V$.

Example 2.11. Let $G = C_3 = \langle (1\ 2\ 3) \rangle$ and V the permutation module of G with basis $B = [v_1, v_2, v_3]$. The subspace $W = \langle v_1 + v_2 + v_3 \rangle$ is a submodule but the subspace $U = \langle v_1 + v_2 \rangle$ is not.

For example, consider the action of $g = (1\ 2\ 3)$ on $v_1 + v_2 \in U$.

$$(v_1 + v_2)g = v_{1g} + v_{2g} = v_2 + v_3 \notin U$$

whereas G acts on W trivially. ◀

3 Lecture 3

3.1 Module and Representation Reducibility

For any module, it is clear that we have two trivial submodules: $0 < V$ and $V < V$. Where $0 = \{0\} \subset V$.

Definition 3.1. Let V be an FG-module. We say that V is irreducible if the only submodules of V are V and 0. Otherwise V is reducible

In 2.11 we showed that the permutation module of C_3 is reducible.

Definition 3.2. Let $\rho : G \to GL(n, F)$ be a representation. We say that ρ is irreducible if the corresponding FG-module (as constructed in 2.1) is irreducible. Otherwise ρ is reducible.

If an FG-module, V is reducible, that is, $0 < W < V$, $0 \neq W \neq V$. Let B_W be a basis for W. If we extend B_W to B a basis of V, then we get the following representation of G:

$$g \mapsto [g]_B = \begin{bmatrix} X_g & 0 \\ Y_g & Z_g \end{bmatrix} \tag{3.1}$$

Where the matrices X_g, Y_g and Z_g are some block matrices and 0 is a block of zeros and X_g has the dimensions $m \times m$ and, in this case, $\dim(W) = m$.

Proposition 3.3. *A representation $\rho : G \to GL(n, F)$ is reducible if and only if with respect to some basis, B, of F^n, $[g]_B$ has the form 3.1 for some $0 < m < \dim(V)$ for all $g \in G$. Then the maps $g \mapsto X_g$ and $g \mapsto Z_g$ are both representations of G.*

Proof. Suppose we have a presentation, $\rho : G \to GL(n, F)$ and a basis B of $V = F^n$ such that $[g]_B$ has the form 3.1 for every $g \in G$. Then consider the subspace $0 \subset W \subset V$ spanned by the first m elements of B. It is clear that $v[g]_B \in W$ for all $v \in W$. Therefore the module induced by ρ is reducible, so ρ is reducible. Now, if we have a reducible representation, then the argument above this proposition shows that with respect to any basis extending B_W, the matrices $[g]_B$ have the required form.
Now, using elementary block matrix multiplication, we get the following for $g, h \in G$:

$$\rho(g)\rho(h) = [g]_B[h]_B = \begin{bmatrix} X_g X_h & 0 \\ Y_g X_h + Z_g Y_h & Z_g Z_h \end{bmatrix} = [gh]_B = \rho(gh)$$

Therefore $X_{gh} = X_g X_h$ and $Z_{gh} = Z_g Z_h$, so the maps $g \mapsto X_g$ and $g \mapsto Z_g$ are both representations of G. ☐

Problem 1. Prove that the example representation of D_8 of degree 2 over $\mathbb{R}$ or $\mathbb{C}$ is irreducible.

3.2 Group Algebras

Recall that an algebra over a field F is a vector space over F equipped with a bilinear product $A \times A \to A$ that is compatible with scalar multiplication.

Definition 3.4. The group algebra over a finite group G over a field F is an algebra[1] of dimension $n = |G|$ over $F = \mathbb{R}$ or $\mathbb{C}$ called FG, with basis $B = G = \{g_1, \ldots g_n\}$.

[1]See Lemma3.6

Where the algebra structure is given by the following for two arbitrary elements of FG, $u = \sum_{g\in G} \lambda_g g$, $v = \sum_{g\in G} \mu_g$, $\lambda_g, \mu_g \in F$ and $\nu \in F$:

(i) $u + v = \sum_{i=1}^{n} (\lambda_i + \mu_i) g_i$

(ii) $\nu \cdot u = \sum_{i=1}^{n} (\nu\lambda_i) g_i$

(iii) $u \cdot v = \sum_{(h,g)\in G\times G} \lambda_g \mu_h (gh)$

This is clearly a vector space.

Example 3.5. Consider $G = C_3 = \{e, a, a^2\} = \langle a | a^3 = e\rangle$ and $F = \mathbb{R}$ or $\mathbb{C}$. Then if we let $u = e - a + 2a^2$, $v = \frac{1}{2}e + 5a$, then:

$$u + v = \frac{3}{2}e + 4a + 2a^2, \quad \frac{1}{3}u = \frac{1}{3}e - \frac{1}{3}a + \frac{2}{3}a^2, \quad uv = \frac{21}{2}e + \frac{9}{2}a - 4a^2$$

◀

Lemma 3.6. *Given a group algebra FG, $r, s, t \in FG$, $\lambda \in F$:*

(I) $rs \in FG$

(II) $(rs)t = r(st)$

(III) $1_G r = r 1_G = r$

(IV) $(\lambda r)s = \lambda(rs)$

(V) $(r + s)t = rt + st$

(VI) $r(s + t) = rs + rt$

(VII) $r0 = 0r = 0$

That is, FG is an associative algebra with unit

Proof. 1,3 and 7 are clear from the definition of FG, 4,5 and 6 follow from the distributive and associative laws of F and 2 follows from associativity in G. □

3.3 The Regular FG-module, FG

Problem 2. $V = FG$ is an FG-module with the group action defined by $v \cdot g = vg$ for $v \in FG$, $g \in G \subset FG$.

Definition 3.7. For a finite group G and $F = \mathbb{R}$ or $\mathbb{C}$, the regular FG-module is FG. The associated module, $g \mapsto [g]_B$ is called the regular representation.

Lemma 3.8. *FG is a faithful module for G over F*

Proof. If $vg = v$ for all $v \in FG$, then specifically, $hg = h$ for all $h \in G$, so $g = 1_G$. □

Example 3.9. For $C = C_3$, over the basis $B = G$, we get:

$$[e]_B = I_3, \quad [a]_B = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad [a^2]_B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

◀

Now, if we have an FG-module, V, then FG acts on V in the following way:

$$v \cdot r = v \cdot \left(\sum_{g \in G} \mu_g g \right) = \sum_{g \in G} \mu_g (v \cdot g)$$

Lemma 3.10. *For $u, v \in V$, $\lambda \in F$, $r, s \in FG$:*

(I) $vr \in FG$

(II) $(vr)s = v(rs)$

(III) $v1 = v$

(IV) $(\lambda v)r = \lambda(vr) = v(\lambda r)$

(V) $v(r + s) = vr + vs$

(VI) $(u + v)r = ur + vr$

(VII) $r0 = v0 = 0$

Proof. I,III and the first part of VII follow from V being an FG-module, the second equality of VII follows from scalar multiplication by 0 in V. The following calculation:

$$\begin{aligned}
(\lambda v)r &= \sum_{g \in G} \mu_g ((\lambda v) g) \\
&= \sum_{g \in G} \mu_g (\lambda (vg)) \\
&= \sum_{g \in G} (\lambda \mu_g)(vg) = v(\lambda r) \\
&= \lambda \sum_{g \in G} \mu_g (vg) \\
&= \lambda (vg)
\end{aligned}$$

proves IV. VI follows from the linearity of the action of G on V. V follows from distributivity of scalar multiplication in V. Finally, to prove II:

$$\begin{aligned} v(rs) &= \sum_{(g,h)\in G\times G} (\mu_g \lambda_h (v(gh))) \\ &= \sum_{h\in G} \lambda_h \sum_{g\in G} \mu_g (gv) h \\ &= \sum_{h\in G} \lambda_h \left(\sum_{g\in G} \mu_g (gv) \right) h \\ &= \sum_{h\in G} \lambda_h (vr) h = (vr)s \end{aligned}$$

□

4 Lecture 4

4.1 Homomorphisms

Definition 4.1. Let V and W be FG-modules. A *homomorphism* of FG-modules is a map $\sigma : V \to W$ which is a linear transformation and also satisfies $(vg)\sigma = (v\sigma)g$ for all $g \in G, v \in V$. The *kernel* and *image* are defined in the obvious way

Equivalently, it is a homomorphism of modules over the ring FG. Indeed:

Problem 3. Suppose $r \in FG$ is an element of the group algebra. Prove that $(vr)\sigma = (v\sigma)r$.

Lemma 4.2. *Let $\sigma : V \to W$ be a homomorphism of FG-algebras. Then the kernel and image of σ are submodules*

Proof. This is a matter of simple checking, which will be left to the reader. □

Example 4.3. Take $\sigma : V \to V$ to be $v \mapsto \lambda v$ for some $\lambda \in F^*$. Then $\ker \sigma = 0, \operatorname{im} \sigma = V$. ◀

Example 4.4. Let $G = S_n$ and $V = \langle v_1, ..., v_n \rangle$ be the permutation module for G over F, and let $W = \langle w \rangle$ be the trivial module. Now define $\sigma : V \to W$ by

$$\sum \lambda_i v_i \mapsto \sum \lambda_i w$$

Then $\ker \sigma = \{\sum \lambda_i v_i \mid \sum \lambda_i = 0\}$ and $\operatorname{im} \sigma = W$. ◀

Definition 4.5. A homomorphism of FG-modules is an *isomorphism* if it is bijective

Remark 1. In class we originally said "if the homomorphism has trivial kernel". However, this is definitely not correct because inclusions are always homomorphisms, but obviously not isomorphisms. ♦

Lemma 4.6. *The inverse of an isomorphism is an isomorphism*

Proof. Once again, this is just an exercise in checking. The details will be left for the reader. □

Some rather obvious invariants of FG-modules (under isomorphism) are dimension and irreducibility.

Lemma 4.7. *V and W are isomorphic if and only if there exists bases $\mathcal{B}_1$ of V and $\mathcal{B}_2$ of W such that*

$$[g]_{\mathcal{B}_1} = [g]_{\mathcal{B}_2}$$

for all g.

Proof. Suppose firstly that V and W are isomorphic, and let $\sigma : V \to W$ be one such isomorphism. Let $\mathcal{B}_1 = \{v_1, ..., v_n\}$ be a basis for V. In particular, it is linearly independent, and it is easy to see that $\mathcal{B}_2 = \{v_1\sigma, ..., v_n\sigma\}$ is also linearly independent. Since V and W are isomorphic, they have the same dimension, and thus $\mathcal{B}_2$ is a basis for W. Since $(vg)\sigma = (v\sigma)g$ for all g and v, the action of g on the basis vectors of both bases are the same, and thus we conclude $[g]_{\mathcal{B}_1} = [g]_{\mathcal{B}_2}$.

Conversely, suppose that the latter hypothesis is satisfied. Let $\{v_1, ..., v_n\}$ be a basis for V and $\{w_1, ..., w_n\}$ be a basis for W. We define a bijective linear map $\sigma : V \to W$ such that $v_i\sigma = w_i$ for each i. Now observe that for each i, we have $v_ig = \lambda_1 v_1 + ... + \lambda_n v_n$ and $w_ig = \lambda_1 w_1 + ... + \lambda_n w_n$, where $(\lambda_1, ..., \lambda_n)$ is the i-th row of $[g]$. This means that

$$(v_ig)\sigma = (\lambda_1 v_1 + ... + \lambda_n v_n)\sigma = \lambda_1 v_1\sigma + ... + \lambda_n v_n\sigma = \lambda_1 w_1 + ... + \lambda_n w_n = w_ig = (v_i\sigma)g$$

and thus σ is a homomorphism of FG-modules. Since it is bijective, it is an isomorphism. □

Theorem 4.8. *Let V be an FG-module with basis $\mathcal{B}_1$ and W an FG-module with basis $\mathcal{B}_2$. Then $W \cong V$ if and only if $g \mapsto [g]_{\mathcal{B}_1}$ and $g \mapsto [g]_{\mathcal{B}_2}$ are equivalent.*

Proof. This follows from the previous Lemma and the fact that two matrices are conjugate (A and B are conjugate if $A = P^{-1}BP$ for some P) if and only if the linear transformations they define differ by a change of basis (that is they define the same transformation but with respect to different bases) □

Example 4.9. Let $G = C_3 = \{e, a, a^2\}$. Let V be the regular representation, that is the natural representation induced by the module $FG = \langle e, a, a^2 \rangle$. Write $B := \{e, a, a^2\}$ as a basis for FG. Then

$$[a]_B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Now let W be the permutation module where $a = (1, 2, 3)$ and C_3 is considered a subgroup of S_3. Write $B' = \{v_1, v_2, v_3\}$ for the basis of W. Then

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

Note that these two modules are isomorphic. ◀

Example 4.10. Let $G = D_4 = \langle a, b \mid a^4 = b^2 = 1, a^b = a^{-1} \rangle$. Now we can act on either F^4 or F^8. On F^4, we have the representation described in Example 1.2. On W, we have the regular representation. Clearly are not isomorphic. ◀

4.2 Sums

We now consider how modules behave with respect to direct sums. Let V be an FG-module and suppose $V = U \oplus W$, where U and W are submodules. Let $\mathcal{B}_1 = \{u_1, ..., u_n\}$ be a basis for U and $\mathcal{B}_2 = \{w_1, ..., w_m\}$ one for W, so that $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_\in$ is a basis for V. Then

$$[g]_{\mathcal{B}} = \begin{pmatrix} [g]_{\mathcal{B}_1} & 0 \\ 0 & [g]_{\mathcal{B}_2} \end{pmatrix}$$

Lemma 4.11. *Let V be an FG-module such that we have the decomposition*

$$V = \bigoplus_{i=1}^{n} U_i$$

Define the projection map $\pi_i : u_1 + u_2 + ... + u_n \mapsto u_i$. Then

(I) *π_i is a homomorphism*

(II) $\pi_i \circ \pi_i = \pi_i$

Proof. Trivial □

Lemma 4.12. *Suppose we have a finite decomposition*

$$V = \sum U_i$$

where the U_i are irreducible. Then V is the direct sum of some subset of the U_i.

Proof. This follows from the fact that the intersection of two distinct irreducible modules is trivial (again, simple checking). □

We will now present an important result

Theorem 4.13 (Maschke's Theorem)**.** *Let G be a finite group, F a field of characteristic 0, V an FG-module and U a submodule. Then there exists some W such that $V = U \oplus W$.*

Proof. We first choose some W_1 such that $V = U \oplus W_1$ as vector spaces. Note that each $v \in V$ can be uniquely decomposed as $v = u + w$, where $u \in U, w \in W_1$. Now define the canonical projection $\sigma : V \to U$ where $v \mapsto u$. Clearly $\ker \sigma = W_1$ and $\operatorname{im} \sigma = U$. However, we note that σ is NOT necessarily a homomorphism of FG-modules. We modify it as follows: Define $\varphi : V \to V$ by

$$v \mapsto \frac{1}{|G|} \sum_{g \in G} vg\sigma g^{-1}$$

We claim that φ IS a homomorphism. Indeed, suppose $x \in G, v \in V$. Then

$$\begin{aligned}(xv)\varphi &= \frac{1}{|G|} \sum_{g \in G} (vx)g\sigma g^{-1} \\ &= \frac{1}{|G|} \sum_{h \in G} vh\sigma h^{-1}x \\ &= \left(\frac{1}{|G|} \sum_{h \in G} vh\sigma h^{-1} \right) x = (v\varphi)x\end{aligned}$$

where the equality

$$\frac{1}{|G|} \sum_{g \in G} (vx)g\sigma g^{-1} = \frac{1}{|G|} \sum_{h \in G} vh\sigma h^{-1}x$$

follows from the change of variables $h = xg$. Clearly φ maps into U, and we now check it is a projection. Indeed, supposing $u \in U$ we have

$$\begin{aligned}(u)\varphi &= \frac{1}{|G|} \sum_{g \in G} ug\sigma g^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} u\sigma gg^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} u \\ &= u\end{aligned}$$

as desired.

Now clearly $U = \operatorname{im}\varphi$ and we define $W := \ker\varphi$. Then for each $v \in V$, write $u := v\varphi \in U$ and $w := v - u \in W$ so that $v = u + w$. It only remains to check that this is unique. To see this, suppose $u' + w' = v = u + w$. Then

$$u' = \varphi(u') = \varphi(v) = \varphi(u) = u$$

which implies the result. □

5 Lecture 5

We begin with consequences of Maschke's theorem.

Example 5.1. Let $G = S_3$, and $V = \langle v_1, v_2, v_3\rangle$ is the permutation module. Let U be the submodule of V defined as $U = \langle v_1 + v_2 + v_3\rangle < V$. Suppose $W_0 = \langle v_1, v_2\rangle$, so that $V = U \oplus W_0$ as subspaces. Define a projection $\phi : V \to U$ by $v_1 \mapsto 0$, $v_2 \mapsto 0$, and $v_3 \mapsto v_1 + v_2 + v_3$. Further, define $\theta : V \to V$, as in proof of Maschke's theorem, so that

$$v\theta = \frac{1}{|G|}\sum_{g\in G} vg\theta g^{-1} = \frac{1}{6}\sum_{g\in S_3} vg\theta g^{-1}.$$

Consider the action of θ on the basis elements v_i, then a short computation shows that

$$v_i\theta = \frac{1}{3}(v_1 + v_2 + v_3), \qquad i = 1, 2, 3.$$

Moreover, we have

$$\ker\theta = \{v \in V : v\theta = 0\} = \left\{\sum_{i=1}^{3}\lambda_i v_i : \sum_{i=1}^{3}\lambda_i = 0\right\}.$$

Hence $V = U \oplus \ker\theta$, is a direct summand of submodules. Moreover, if $\mathcal{B} = [v_1 + v_2 + v_3, v_1, v_2]$ is a basis for V, and $\mathcal{B}' = [v_1 + v_2 + v_3, v_1 - v_2, v_2 - v_3]$ is another, one has

$$[g]_{\mathcal{B}} = \begin{pmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}, \qquad [g]_{\mathcal{B}'} = \begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

◀

In fact, it follows from Maschke's theorem that if we choose a basis $\mathcal{B}$ for V such that

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

then there exists a basis $\mathcal{B}'$ for V such that

$$[g]_{\mathcal{B}'} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}.$$

Definition 5.2. Let V be a FG-module, V is said to be **completely reducible** if $V = U_1 \oplus \cdots \oplus U_r$ with each U_i an irreducible FG-module.

Theorem 5.3. *Suppose G is a finite group, and $F = \mathbb{R}, \mathbb{C}$. Then every FG-module is completely reducible*

Proof. Induction using Maschke's theorem. □

Lemma 5.4. *Suppose G is a finite group, $F = \mathbb{R}, \mathbb{C}$, and V a FG-module. If U is a FG-submodule, then there exists a surjective FG-homomorphism from V onto U.*

Proof. By Maschke's theorem, there exists a complementary submodule W to U such that $V = U \oplus W$. Thus, defining $\pi : V \to U$ by $u + w \mapsto u$ gives the result. □

Example 5.5. Take

$$G = \left\langle \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\rangle$$

and $V = \mathbb{C}^2$. Then V is not completely reducible. ◀

Example 5.6. Let $G = C_p = \langle a \mid a^p = 1 \rangle$ where p is prime, and take the representation

$$a^j \mapsto \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}, \qquad 0 \leq j \leq p-1$$

over the finite field $F = \mathbb{Z}_p$. If $V = \langle v_1, v_2 \rangle$ is the FG-module of the representation and $U = \langle v_2 \rangle$, then there does not exist a submodule $W < V$ such that $V = U \oplus W$. ◀

The previous two examples show that the assumptions of Maschke's theorem are required, and cannot be relaxed.

5.1 Schur's Lemma

Theorem 5.7 (Schur's lemma)**.** *Suppose V and W are irreducible $\mathbb{C}G$-modules.*

(I) *If $\theta : V \to W$ is a $\mathbb{C}G$-homomorphism, then θ is either a $\mathbb{C}G$-isomorphism or the zero homomorphism.*

(II) *If $\theta : V \to V$ is a $\mathbb{C}G$-isomorphism, then θ is scalar multiple of the identity endomorphism of V.*

Proof. (I): Suppose that $v\theta \neq 0$ for some $v \in V$, then the image of θ is not trivial, $\operatorname{im}\theta \neq \{0\}$. However, $\operatorname{im}\theta$ is a submodule of W, and so the irreducibility of W forces $\operatorname{im}\theta = W$. Likewise, as the kernel of θ is a submodule of V, but not all of V, we have $\ker\theta = \{0\}$ as V is irreducible. Therefore, θ is a bijective $\mathbb{C}G$-homomorphism, and so it is a $\mathbb{C}G$-isomorphism.

(II): Suppose θ is a $\mathbb{C}G$-isomorphism. Then as $\mathbb{C}$ is algebraically closed, θ has an eigenvalue $\lambda_v \in \mathbb{C}$ with $v\theta = \lambda_v v$ for some $v \in V$. Now, as $\ker(\theta - \lambda_v 1_V) \neq \{0\}$ is a submodule of V, V being irreducible implies that $\ker(\theta - \lambda_v 1_V) = V$. Therefore, $w(\theta - \lambda_v 1_V) = 0$ for all $w \in V$, and so $\theta = \lambda 1_V$ as required. $\square$

Further, we actually have a converse to the second statement of Schur's lemma.

Proposition 5.8. *Let V be a nontrivial $\mathbb{C}G$-module, and suppose that every $\mathbb{C}G$-homomorphism from V to V is a scalar multiple of the identity endomorphism of V. Then V is irreducible.*

Proof. Suppose V is reducible. Then there exists a nontrivial submodule U of V such that, by Maschke's theorem, $V = U \oplus W$ with W also a submodule of V. Defining $\pi : V \to V$ by $u + w \mapsto u$ gives a $\mathbb{C}G$-homomorphism that is not a multiple of the identity endomorphism. A contradiction. $\square$

We now interpret Schur's lemma as representation statement.

Lemma 5.9. *Let $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ be a representation. Then ρ is irreducible if, and only if, every $n \times n$ matrix A which satisfies $(g\rho)A = A(g\rho)$ for all $g \in G$, has the form $A = \lambda I_n$.*

Proof. Result follows from Schur's lemma and its partial converse. $\square$

Example 5.10. Suppose $G = C_3 = \langle a \mid a^3 = 1\rangle$, and $\rho : G \to \mathrm{GL}(2, \mathbb{C})$ is the representation defined by

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

Let

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

Then it is clear that $A(g\rho) = (g\rho)A$ for all $g \in G$. As A is not a scalar multiple of the identity, the representation is reducible. ◀

Example 5.11. Suppose $G = D_5 = \langle a, b \mid a^5 = 1, b^2 = 1, a^b = a^{-1}\rangle$. Set $\omega = e^{2\pi i/5}$. Let $\rho : G \to \mathrm{GL}(2, \mathbb{C})$ be the representation defined by

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

If

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

commutes with $a\rho$ and $b\rho$; one calculates that

$$A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} = \alpha I_n,$$

and so the representation is irreducible. ◀

Lemma 5.12. *Let G be a finite abelian group. Then every irreducible $\mathbb{C}G$-module has dimension 1.*

Proof. Choose $x \in G$, then $v(gx) = v(xg)$ for all $g \in G$, and so $v \mapsto vx$ is a $\mathbb{C}G$-homomorphism. It is actually an isomorphism with inverse $v \mapsto vx^{-1}$. Hence by Schur this isomorphism is a scalar multiple of the identity, say $\lambda_x 1_V$. Thus $vx = \lambda_x 1_V$ for all $v \in V$ and the group action by G is just usual scalar multiplication. This means that every subspace is a submodule. However, V is irreducible and so has no non-trivial submodules; which forces $\dim V = 1$. □

6 Lecture 6

Continuing our discussion of the representations of abelian groups, we provide a stronger theorem in which we construct these 1-dimensional representations by mapping group elements to roots of unity. But first recall the Fundamental Theorem of Abelian Groups which states that any finite abelian group G is isomorphic to the direct sum of cyclic groups

$$G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$$

where $n_i \mid n_{i+1}$ for all $1 \leq i \leq r-1$. Note that if $C_i = \langle g_i \rangle$ then we can write $G = \langle g_1, \ldots, g_r \rangle$ and g_i has order n_i.

We define a homomorphism ρ from G to $\mathbb{C}$ by taking $g_i \mapsto \lambda_i$ where λ_i is the n_i-th root of unity. This defines a representation and is specified by roots of unity $\lambda_1, \cdots, \lambda_r$. Thus for the representation ρ defined by roots of unity $\lambda_1, \ldots, \lambda_r$ we write $\rho = \rho_{\lambda_1, \ldots, \lambda_r}$.

Theorem 6.1. *Suppose $G \simeq C_{n_1} \times \cdots \times C_{n_r}$ for cyclic groups C_{n_i} of order n_i. The representation $\rho_{\lambda_1,\ldots,\lambda_r}$ of G is irreducible of degree 1. There are $|G|$ many such representations and every irreducible representation of G over $\mathbb{C}$ is equivalent to one of these.*

Example 6.2. Take $G = \langle a \mid a^n = 1 \rangle$ and $\omega = e^{2\pi i/n}$. The irreducible representations of G are ρ_{ω^j} for $0 \leq j \leq n-1$ defined by

$$a^k \rho_{\omega^j} = \omega^{jk}, \quad 0 \leq k \leq n-1.$$

◀

6.1 Application of Schur's to $\mathbb{C}G$

Definition 6.3. If G is a finite group then we define the center of the group algebra $Z(\mathbb{C}G)$ by

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

We now state some simple properties of the center:

1. $Z(\mathbb{C}G)$ is a subspace of $\mathbb{C}G$.
2. If G is abelian then $Z(\mathbb{C}G) = \mathbb{C}Z(G)$.
3. If H is a normal subgroup of G then $\sum_{h \in H} h \in Z(\mathbb{C}G)$.

We provide a simple proof for the last statement.

Proof. Take $z = \sum_{h \in H} h$ and $g \in G$. We then have

$$z^g = \sum_{h \in H} h^g = z.$$

because H is normal and hence fixed by conjugation of elements in G. □

Example 6.4. Take $G = S_3 = \langle a = (1\ 2\ 3), b = (1\ 2)\rangle$. Then $\sum_{g \in G} \in Z(\mathbb{C}G)$. ◀

Lemma 6.5. *Let V be an irreducible $\mathbb{C}G$-module and let $z \in Z(\mathbb{C}G)$. There exists $\lambda \in \mathbb{C}$ such that $vz = \lambda v$ for all $v \in V$.*

Proof. For all $r \in \mathbb{C}G$ and $v \in V$ we know $vrz = vzr$. Thus the mapping $v \mapsto vz$ is a $\mathbb{C}G$-homomorphism from V to V. The result then follows by Schur. □

Remark 2. Note that $\mathbb{C}G$ is a faithful module. ♦

Lemma 6.6. *If there exists a faithful, irreducible $\mathbb{C}G$-module then $Z(G)$ is cyclic.*

Proof. Let V be an irreducible, faithful $\mathbb{C}G$-module and take $z \in Z(G) \subset Z(\mathbb{C}G)$. There exists $\lambda_z \in \mathbb{C}$ such that $vz = \lambda_z v$ for all $v \in V$. But since V is faithful the mapping $z \mapsto \lambda_z$ is injective from $Z(G)$ to $\mathbb{C}^\times$ and so $Z(G) \simeq \{\lambda_z \mid z \in Z(G)\}$ is a finite subgroup of $\mathbb{C}^\times$. All of which are cyclic. □

Example 6.7. $\mathbb{Z}_4$ has a faithful, irreducible representation by taking 1 to the 4-th root of unity. However $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no faithful irreducible representation as its center is not cyclic. ◀

Remark 3. Note that the converse is not true in general. There exists groups with cyclic centers but no faithful, irreducible representations. See Frobenius Groups. ♦

Lemma 6.8. *Suppose G finite and every irreducible $\mathbb{C}G$-module has dimension 1. Then G is abelian.*

Proof. Since $\mathbb{C}G$ is is a $\mathbb{C}G$-module and it is completely reducible, we can decompose it as follows

$$\mathbb{C}G = \bigoplus_{i=1}^{|G|} V_i$$

where each V_i is one-dimensional. For any $v_i \in V_i$ and $x, y \in G$, note that

$$v_i xy = \lambda_x v_i y = \lambda_y \lambda_x v_i = \lambda_x \lambda_y v_i = v_i yx$$

Since the v_i form a basis for $\mathbb{C}G$ this means $vxy = vyx$ for all $v \in \mathbb{C}G$ and $x, y \in G$. Since $\mathbb{C}G$ is faithful, the result follows. □

6.2 The Group Algebra and Irreducible Modules

Lemma 6.9. *Let V, W be $\mathbb{C}G$-modules and $\theta : V \to W$ is a $\mathbb{C}G$-homomorphism. There exists a submodule $U < V$ such that $V = \ker\theta \oplus U$ and $U \simeq \operatorname{im}\theta$*

Proof. We apply Maschke's theorem to $\ker\theta < V$ and obtain submodule $U < V$ such that $V = \ker\theta \oplus U$. Now define the map $\overline{\theta} : U \to \operatorname{im}\theta$ by $u \mapsto u\theta$ which is a homomorphism because it is the restriction of θ to a subspace. The kernel of $\overline{\theta}$ is trivial as $\ker\overline{\theta} = \ker\theta \cap U = \{0\}$. And $\operatorname{im}\theta = \operatorname{im}\overline{\theta}$ because if $w \in \operatorname{im}\theta$ then $w = v\theta$ for some $v \in V$ and $v = k + u$ for some $u \in U$ and $k \in \ker\theta$. We then have

$$w = v\theta = (u + k)\theta = u\theta = u\overline{\theta} \in \operatorname{im}\overline{\theta}.$$

Finally, by the first isomorphism theorem we obtain

$$U \simeq U/\ker\overline{\theta} \simeq \operatorname{im}\overline{\theta} = \operatorname{im}\theta.$$

□

7 Lecture 7

7.1 The Group Algebra and Irreducible Modules: Part II

Definition 7.1. For V, a $\mathbb{C}G$-module, U an irreducible $\mathbb{C}G$-module, U is called a composition factor for V if V has a $\mathbb{C}G$-submodule isomorphic to U.

Lemma 7.2. *Let V be a $\mathbb{C}G$-module, suppose we have a finite decomposition into into a direct sum of irreducible $\mathbb{C}G$-modules:*

$$V = \bigoplus_{i=1}^{n} U_i$$

Then, if $0 < U < V$ is an irreducible, $\mathbb{C}G$-submodule of V, then $U \simeq U_i$ for some $1 \leq i \leq n$.

Proof. Consider the maps $\pi_i : U \to U_i$, since each $\pi_i : V \to U_i$ is a $\mathbb{C}G$-homomorphism, and since U is non-trivial, it is clear that not all the π_i are the zero map, let π_j be such a projection, then by Schur, $\pi_j : U \to U_j$ is a $\mathbb{C}G$-isomorphism. □

Theorem 7.3. *Let the following be a decomposition of the regular representation into irreducible $\mathbb{C}G$-modules:*

$$\mathbb{C}G = \bigoplus_{i=1}^{n} U_i$$

Then every irreducible $\mathbb{C}G$-module is isomorphic to U_i for some $1 \leq i \leq n$

Proof. Let W be an irreducible $\mathbb{C}G$-module, let $0 \neq w \in W$, then $wG = \{wr : r \in \mathbb{C}G\}$ is a $\mathbb{C}G$-submodule of W. However, W is irreducible, so $W = wG$. Define $\theta : \mathbb{C}G \to W$ by $r\theta = wr$ for $r \in \mathbb{C}G$, then θ is a linear $\mathbb{C}G$-homomorphism by 3.10 and $\operatorname{im}\theta = W$. So $\mathbb{C}G = \ker\theta \oplus U$, where $U \simeq \operatorname{im}\theta \simeq W$ by 6.9. Now W is irreducible, so U is irreducible, so by 7.2, $U \simeq U_i \simeq W$ for some $1 \leq i \leq n$. □

Now for a finite group G, we can characterise all irreducible $\mathbb{C}G$-modules by decomposing $\mathbb{C}G$.

Example 7.4. Let $G = C_3 = \langle a | a^3 = 1\rangle$, then let $\omega = e^{\frac{2\pi i}{3}}$ be a primitive 3rd root of unity and let the following be elements of $\mathbb{C}G$:

$$v_1 = 1 + a + a^2, \qquad v_2 = 1 + \omega^2 a + \omega a^2, \qquad v_3 = 1 + \omega a + \omega^2 a^2$$

We have $(v_1)a = v_1$, $(v_2)a = \omega + a + \omega^2 a^2 = \omega v_2$ and $(v_3)a = \omega^2 + a + \omega a = \omega^2 v_3$ Therefore, $V_i = \langle v_i \rangle < \mathbb{C}G$ for $i = 1, 2, 3$ are all irreducible submodules of $\mathbb{C}G$.

Furthermore, it is clear that $\{v_1, v_2, v_3\}$ forms a basis for $\mathbb{C}G$, hence $\mathbb{C}G = V_1 \oplus V_2 \oplus V_3$. ◄

Example 7.5. Let $G = D_6 = \langle a, b | a^3 = 1, a^b = a^{-1}\rangle$ be the dihedral group of order 6, and let $\omega = e^{2\pi i/3}$ be a third root of unity. Define $v_i \in \mathbb{C}G$ by $v_i a = \omega^i v_i$, then

$$\begin{aligned} v_0 &= 1 + a + a^2, \\ v_1 &= 1 + \omega^2 a + \omega a^2, \\ v_2 &= 1 + \omega a + \omega^2 a^2. \end{aligned}$$

Further define $u_i = bv_i$ for all $i = 0, 1, 2$. Then it follows that $\langle v_i \rangle$ and $\langle w_i \rangle$ are $\mathbb{C}\langle a \rangle$-modules for all i. Further, a short computation shows that

$$\langle v_0, u_0 \rangle, \quad \langle v_1, u_2 \rangle, \quad \langle v_2, u_1 \rangle$$

are $\mathbb{C}\langle b \rangle$-modules. Hence, we see that

$$\begin{aligned} U_1 &= \langle v_0 + u_0 \rangle, \\ U_2 &= \langle v_0 - u_0 \rangle, \\ U_3 &= \langle v_1, u_2 \rangle, \\ U_4 &= \langle v_2, u_1 \rangle, \end{aligned}$$

are irreducible $\mathbb{C}G$-submodules. It is clear that $U_3 \simeq U_4$ via the map that sends $v_1 \mapsto u_1$ and $u_2 \mapsto v_2$. Finding the representations of each U_i we have

$$\begin{aligned}
\rho_1 &: a \mapsto (1), \quad b \mapsto (1), \\
\rho_2 &: a \mapsto (1), \quad b \mapsto (-1), \\
\rho_3 &: a \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\end{aligned}$$

Hence U_1, U_2, and U_3 are non-isomorphic irreducible $\mathbb{C}G$-submodules. Moreover, we have

$$\mathbb{C}G = \underbrace{U_1}_{\text{trivial}} \oplus U_2 \oplus \underbrace{U_3 \oplus U_4}_{\text{isomorphic}}.$$

◀

7.2 The Vector Space of $\mathbb{C}G$-homomorphisms

Definition 7.6. Let V, W be $\mathbb{C}G$-modules, then define $H = \mathrm{Hom}_{\mathbb{C}G}(V, W) = \{\theta : V \to W : \theta \text{ is a } \mathbb{C}G \text{ homomorphism}\}$.

We can then define addition and scalar multiplication operations on this set for $\theta, \phi \in H$, $\lambda \in \mathbb{C}$ as follows:

$$v(\theta + \phi) := v\theta + v\phi, \qquad v(\lambda\theta) = \lambda(v\theta)$$

Lemma 7.7. *The space H with the operations defined above is a vector space over $\mathbb{C}$.*

Proof. Clear from the definition, note that the zero homomorphism is: $v0 = 0_W$. □

Lemma 7.8. *For irreducible $\mathbb{C}G$-modules, V, W,*

$$\dim(H) = \begin{cases} 1 & V \simeq W \\ 0 & V \not\simeq W \end{cases}$$

Proof. If $V \not\simeq W$, then it follows that $\theta = 0$ for all $\theta \in H$ by Schur.

Now, suppose $V \simeq W$ and let $\theta : V \to W$ be an isomorphism. Now, let $\phi \in H$, we have that $\phi\theta^{-1} : V \to V$ is a homomorphism, so by Schur, $\phi\theta^{-1} = \lambda \,\mathrm{Id}_V$, so for $v \in V$, $v\phi\theta^{-1} = \lambda v \implies v\phi\theta^{-1}\theta = v\phi = (\lambda v)\theta = \lambda(v\theta)$, therefore $\phi = \lambda\theta$, so $\dim H = 1$. □

Proposition 7.9. *Given V, V_1, V_2, W, W_1, W_2 $\mathbb{C}G$-modules,*

1. $\dim \mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2) = \dim \mathrm{Hom}_{\mathbb{C}G}(V, W_1) + \dim \mathrm{Hom}_{\mathbb{C}G}(V, W_2)$
2. $\dim \mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W) = \dim \mathrm{Hom}_{\mathbb{C}G}(V_1, W) + \dim \mathrm{Hom}_{\mathbb{C}G}(V_2, W)$

Proof. I will prove the first statement and the conversion of the proof ot the second statement is left as a simple exercise.

Firstly, we define the projection homomorphisms: $\pi_i : W_1 \oplus W_2 \to W_i$ defined by $(w_1 + w_2)\pi_i = w_i$. Now, if $\theta \in \mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2)$, we have that $\theta\pi_i \in \mathrm{Hom}_{\mathbb{C}G}(V, W_i)$.

Define a linear map $f : \mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2) \to \mathrm{Hom}_{\mathbb{C}G}(V, W_1) \oplus \mathrm{Hom}_{\mathbb{C}G}(V, W_2)$ by $\theta \mapsto \theta\pi_1 \oplus \theta\pi_2$ then it is clear that the following map is an inverse of f:

$$v(\theta_1 \oplus \theta_2)f^{-1} = v\theta_1 + v\theta_2$$

therefore we have an isomorphism of vector spaces, $\mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2) \simeq \mathrm{Hom}_{\mathbb{C}G}(V, W_1) \oplus \mathrm{Hom}_{\mathbb{C}G}(V, W_2)$, giving us $\dim \mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2) = \dim \mathrm{Hom}_{\mathbb{C}G}(V, W_1) \oplus \mathrm{Hom}_{\mathbb{C}G}(V, W_2) = \dim \mathrm{Hom}_{\mathbb{C}G}(V_1, W) + \dim \mathrm{Hom}_{\mathbb{C}G}(V_2, W)$ □

Corollary 7.9.1. *For $V_1, \ldots V_n$, $W_1, \ldots W_m$, if $V = \bigotimes_{i=1}^n V_i$ and $W = \bigotimes_{i=1}^m W_i$*

$$\dim H = \sum_{i=1}^{n} \sum_{j=1}^{m} \dim \mathrm{Hom}_{\mathbb{C}G}(V_i, W_j)$$

Corollary 7.9.2. *Suppose*

$$V = \bigoplus_{j=1}^{n} U_j$$

Then for any irreducible module W

$$\dim \mathrm{Hom}(V, W) = \dim \mathrm{Hom}(W, V) = |\{j \mid U_j \cong W\}|$$

Example 7.10. Recall that

$$\mathbb{C}D_3 = \bigoplus_{i=1}^{4} U_i$$

where $U_3 \cong U_4$. Then

$$\dim \mathrm{Hom}(\mathbb{C}D_3, U_3) = 2$$

◀

8 Lecture 8

We continue the discussion last lecture about $\mathrm{Hom}(U, V)$.

Lemma 8.1. *Let V, W be two $\mathbb{C}G$-modules such that $\mathrm{Hom}(V, W)$ is nonzero. Then V and W share a composition factor.*

Proof. Supopse we have a morphism $\theta : V \to W$. Then there exists some $v \in V$ such that $v\theta \neq 1$. Now v is contained in some irreducible submodule, say V_0. Then $V_0\theta \cong V_0$. □

Lemma 8.2. *Let U be a $\mathbb{C}G$-module. Then*

$$\dim \mathrm{Hom}(\mathbb{C}G, U) = \dim U$$

.

Proof. Fix a basis $\{u_1, \ldots, u_n\}$ for U and define $\varphi_i : \mathbb{C}G \to U$ as $r \mapsto u_i r$. We claim the φ_i form a basis for $\mathrm{Hom}(\mathbb{C}G, U)$. Indeed, let $\varphi \in \mathrm{Hom}(\mathbb{C}G, U)$ and suppose

$$(1)\varphi = \sum_{i=1}^{n} \lambda_i u_i$$

Then for all $r \in \mathbb{C}G$ we have

$$(r)\varphi = (1)\varphi r = (\sum_{i=1}^{n} \lambda_i u_i) r = \sum_{i=1}^{n} \lambda_i u_i r = \sum_{i=1}^{n} \lambda_i (r)\varphi_i$$

where the first equality follows from Problem 3 □

Theorem 8.3. *Suppose*

$$\mathbb{C}G = \bigoplus_{j=1}^{n} V_j$$

and U is an irreducible module. Then the number of j such that $V_j \cong U$ is exactly $\dim U$

Proof. Combine Lemma 8.2 and Corollary 7.9.2 □

Example 8.4. Recall that

$$\mathbb{C}D_3 = \bigoplus_{i=1}^{4} U_i$$

where $U_3 \cong U_4$ but $U_1 \ncong U_2$. Then U_1 and U_2 occur once whereas U_3 occurs twice, consistently with the theorem. ◀

Theorem 8.5. *Let $V_1, ..., V_n$ denote a complete set of irreducible modules that are pairwise non-isomorphic. Then*

$$\sum_{i=1}^{n} (\dim V_i)^2 = |G|$$

Proof. Suppose

$$\mathbb{C}G = \bigoplus_{j=1}^{N} U_j$$

where for each V_i there are exactly $\dim V_i$ of the U_j isomorphic to V_i. Thus we have

$$|G| = \dim \mathbb{C}G = \sum_{i=1}^{N} \sum_{j=1}^{\dim V_i} \dim U_j = \sum_{i=1}^{N} \sum_{j=1}^{\dim V_i} \dim V_i = \sum_{i=1}^{n} (\dim V_i)^2$$

□

Observe that $\mathbb{C}G$ always has a trivial submodule, namely the module spanned by $\sum_{g \in G} g$.

Example 8.6. Note that $|D_3| = 6$ and $6 = 1^2 + 1^2 + 2^2$. This is the only way; indeed, if all irreducible submodules are of dimension 1, then D_3 would be abelian, which is obviously false. ◀

9 Lecture 9

9.1 Group Theoretic Diversion

Suppose G is a group. We define a equivalence relation on G called **conjugacy** by

$$x \sim y \iff y = x^y = g^{-1}xg, \quad \text{for some } g \in G.$$

The equivalence class

$$x^G = G^{-1}yG = \{g^{-1}xg \mid g \in G\},$$

is called the **conjugacy class** of x.

Lemma 9.1. *Every group is a union of conjugacy classes and distinct classes are disjoint.*

Proof. Every equivalence relation on a set corresponds to a partition of said set. □

Example 9.2. For any group G, $1^G = \{1\}$ is a conjugacy class in G. More generally, if $x \in Z(G)$ then $xg = gx$ for all $g \in G$; from which it follows that $x^G = \{x\}$. ◀

Example 9.3. Let $G = D_6$ the dihedral group of 6 elements, generated by the elements a, b. Then $a^G = \{a, a^2\}$, and $b^G = \{b, ab, a^2b\}$. Hence $D_6 = 1^G \amalg a^G \amalg b^G$. ◀

Example 9.4. If G is an abelian group, then for all $x \in G$, $x^G = \{x\}$. This follows from a previous example as G is abelian if, and only if, $G = Z(G)$. ◀

Lemma 9.5. *Suppose that $x, y \in G$ with $x \sim y$, then $x^n \sim y^n$ for all $n \in \mathbb{N}$. In particular, $|x| = |y|$.*

Proof. As $x \sim y$ there exists $g \in G$ such that $x = g^{-1}yg$. By induction, it follows that $x^n = g^{-1}y^ng$ which shows that $x^n \sim y^n$. To see that the orders are equal, note that $x^n = 1$ if, and only if $g^{-1}y^ng = 1$. Hence $y \in 1^G = \{1\}$ and so $y^n = 1$. □

Suppose $x \in G$. Define the **centraliser** of x in G to be the set

$$C_G(x) = \{g \in G \mid xg = gx\} = \{g \in G \mid x^g = x\},$$

i.e. the set of $g \in G$ which fix x under conjugation. It is clear that $C_G(x) \leq G$

Theorem 9.6 (Orbit-stabiliser)**.** *Suppose G is a finite group and $x \in G$. Then $|x^G| = |G : C_G(x)| = |G|/|C_G(x)|$, and in particular $|x^G| \mid |G|$.*

Proof. First we have the chain of equivalences:

$$\begin{aligned} g^{-1}xg = h^{-1}xh &\iff hg^{-1}x = xhg^{-1} \\ &\iff hg^{-1} \in C_G(x) \\ &\iff C_G(x)g = C_G(x)h. \end{aligned}$$

Hence let Λ denote the set of right cosets of $C_G(x)$ in G, and define the function

$$\begin{aligned} &f : x^G \to \Lambda \\ &g^{-1}xg \mapsto C_G(x). \end{aligned}$$

Then f is well-defined by the previous working. Moreover, the previous working also shows that f is injective, and it is clearly surjective. Thus $|G : C_G(x)|$. ☐

Observe that

$$\begin{aligned} |x^G| = 1 &\iff g^{-1}xg = x \quad \forall g \in G \\ &\iff xg = gx \quad \forall g \in G \\ &\iff x \in Z(G). \end{aligned}$$

Theorem 9.7 (Class equation)**.** *Let G be a finite group and suppose $G = \coprod_i x_i^G$. Then*

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|,$$

where $|x_i^G| = |G : C_G(x_i)|$ and both components divide $|G|$.

Proof. As G is a disjoint union of conjugacy classes, we have

$$|G| = \left| \coprod_i x_i^G \right| = \sum_i |x_i^G|.$$

Finally use the fact that $x \in Z(G)$ if, and only if, $|x^G| = 1$. The fact $|x_i^G| = |G : C_G(x_i)|$, and both components divide $|G|$ follow from the orbit-stabiliser theorem. ☐