Introduction to Representation Theory

Konstantin Ardakov

1. Representations of finite groups

Group representation theory is a marriage of Group Theory and Linear Algebra. Its aim is to study *all* the ways in which a given group can arise as a group of symmetries of some vector space.

Notation 1.1. Throughout this course, k will denote a field, and all vector spaces are understood to be k-vector spaces. Recall that the *general linear group* of a k-vector space V is the group $\mathrm{GL}(V)$ of invertible k-linear transformations $V \to V$ with the operation of composition.

Definition 1.2. Let G be a finite group and let V be a finite dimensional vector space over k. A *representation* of G on V is a group homomorphism

$$\rho : G \to \mathrm{GL}(V).$$

The *degree* of the representation is $\dim V$.

If we need to be more precise about the ground field of scalars, we will say "ρ is a k-representation of G". Here are some examples from Geometry.

Example 1.3.

(a) The cyclic group $G = \langle g \rangle$ of order 2 acts on $V = k$ by negation: $\rho(g) = -1$ gives a representation of G of degree 1.

(b) Let G be the symmetry group of a triangle: $G = D_6 = \{e, r, r^2, s, sr, sr^2\}$ and let $k = \mathbb{R}$. Then G acts by $\mathbb{R}$-linear transformations on the plane $V = \mathbb{R}^2$. This gives rise to a representation

$$\rho : G \to \mathrm{GL}(V)$$

where $\rho(r)$ is the rotation through $2\pi/3$ and $\rho(s)$ is the reflection in the y-axis.

(c) The symmetry group of the regular n-gon $G = D_{2n}$ acts on $V = \mathbb{R}^2$ by $\mathbb{R}$-linear transformations, giving a natural representation of G of degree 2.

(d) Let $k = \mathbb{R}$, let $X \subset \mathbb{R}^3$ be the set of vertices of a cube centred at the origin, and let G be the stabiliser of X in the rotation group $SO_3(\mathbb{R})$. Then from your Prelims M1 course you know that G is isomorphic to the symmetric group S_4. In this way, we obtain a degree 3 representation

$$\rho : S_4 \to \mathrm{GL}(\mathbb{R}^3)$$

of this symmetric group.

One may view representations as a "linearisation" of the notion of a group action on a set. This gives a large class of examples of representations, as follows.

Definition 1.4. Let X be a finite set. The *free vector space on* X, is the set

$$kX := \left\{ \sum_{x \in X} a_x \, x : a_x \in k \right\}$$

of *formal linear combinations* of members of X with coefficients a_x lying in k. The addition and scalar multiplication operations on kX are the evident ones.

Note that X is naturally a basis for kX.

Definition 1.5. Let X be a finite set equipped with a left action of the finite group G. Each $g \in G$ defines a permutation $\rho(g) : X \to X$, given by $\rho(g)(x) = g \cdot x$. This permutation extends uniquely to an invertible linear map $\rho(g) : kX \to kX$:

$$\rho(g) \left(\sum_{x \in X} a_x x \right) = \sum_{x \in X} a_x \, g \cdot x.$$

Since $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and all $x \in X$ one checks easily that $\rho(g)\rho(h) = \rho(gh)$ in $\mathrm{GL}(kX)$ for all $g, h \in G$. Thus $\rho : G \to \mathrm{GL}(kX)$ is a representation, called the *permutation representation* (associated with X).

Here is an example from Galois Theory.

Example 1.6. Let $k = \mathbb{Q}$ be the field of rational numbers and let F be a finite field extension of k (so that $\dim_k F < \infty$). Let G be the group of all field automorphisms of F. Then every $g \in G$ is a k-linear map $g : F \to F$, and one of the main results of Galois Theory tells us that G is a finite group. Then the inclusion $G \hookrightarrow \mathrm{GL}(F)$ gives a k-linear representation of G of degree $\dim_k F$.

For example, F could be the splitting field $\mathbb{Q}(\sqrt{2}, e^{\frac{2\pi i}{3}})$ of the polynomial $x^3 - 2$. Then G is the symmetric group S_3 and this gives a $\mathbb{Q}$-linear representation $\rho : S_3 \to \mathrm{GL}(F)$ of degree 6.

The study of representations of Galois groups form a major part of modern Algebraic Number Theory, for example through the Langlands Programme.

Definition 1.7. The representation $\rho : G \to \mathrm{GL}(V)$ is *faithful* if $\ker \rho = \{1\}$.

One reason group representations are interesting to a group-theorist is the following. Given a representation $\rho : G \to \mathrm{GL}(V)$, it is either faithful, or not. If it is faithful, then G is isomorphic to its image in $\mathrm{GL}(V)$ which, using matrix representations below, is easy to compute with. Otherwise $\ker \rho$ is a proper *normal* subgroup of G and $G/\ker \rho$ is isomorphic to $\rho(G)$.

Definition 1.8. Let G be a finite group. A *matrix representation* is a group homomorphism $\rho : G \to \mathrm{GL}_n(k)$, where $\mathrm{GL}_n(k) = M_n(k)^\times$ denotes the group of invertible matrices under matrix multiplication.

There is a close connection between representations and matrix representations. Recall the following from Part A Linear Algebra.

Definition 1.9. Let $\mathcal{B} := \{v_1, \dots, v_n\}$ be a basis for V and let $\phi : V \to V$ be a linear map. The *matrix of ϕ with respect to $\mathcal{B}$* is ${}_{\mathcal{B}}[\phi]_{\mathcal{B}} = (a_{ij})_{i,j=1}^n$ where

$$\phi(v_j) = \sum_{i=1}^n a_{ij} v_i \quad \text{for all} \quad j = 1, \dots, n.$$

Remark 1.10. Let V be a vector space V with basis $\mathcal{B}$.

(a) The map $\phi \mapsto {}_{\mathcal{B}}[\phi]_{\mathcal{B}}$ gives an isomorphism of groups $\mathrm{GL}(V) \xrightarrow{\cong} \mathrm{GL}_n(k)$.

(b) Every representation $\rho : G \to \mathrm{GL}(V)$ gives rise to a matrix representation $\rho_{\mathcal{B}} : G \to \mathrm{GL}_n(k)$ given by

$$\rho_{\mathcal{B}}(g) := {}_{\mathcal{B}}[\rho(g)]_{\mathcal{B}} \quad \text{for all} \quad g \in G.$$

(c) Conversely, every matrix representation $\sigma : G \to \mathrm{GL}_n(k)$ defines a representation $\underline{\sigma} : G \to \mathrm{GL}(k^n)$ on the space k^n of column vectors, by letting $\underline{\sigma}(g) : k^n \to k^n$ be the k-linear map given by

$$\underline{\sigma}(g)(v) = \sigma(g)v \quad \text{for all} \quad g \in G, v \in k^n$$

where $\sigma(g)v$ means the multiplication of the $n \times n$ matrix $\sigma(g)$ by the $n \times 1$ column vector v. We will sometimes abuse notation and simply wrote σ for $\underline{\sigma}$.

Example 1.11. Let $G = S_3$ act on $X = \{e_1, e_2, e_3\}$ by permutations of indices. We obtain a degree 3 permutation representation $\rho : G \to \mathrm{GL}(kX)$. Since

$$(123) \cdot e_1 = e_2, \quad (123) \cdot e_2 = e_3, \quad (123) \cdot e_3 = e_1$$

we see that

$$\rho_X((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Similarly, one can calculate

$$\rho_X((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Warning: in this course, permutations in S_n are multiplied from *right to left*, in contrast to the conventions in Prelims M1. Thus, for example, we have in S_3

$$(123) \cdot (12) = (13).$$

This way of writing and multiplying permutations is necessary to ensure that the natural action of S_n on $\{1, \cdots, n\}$ given by $\sigma \cdot n = \sigma(n)$ is a left action: it satisfies the axiom $g \cdot (h \cdot x) = (gh) \cdot x$ as opposed to a right action $(x \cdot g) \cdot h = x \cdot (gh)$.

Definition 1.12. Let $\rho : G \to \mathrm{GL}(V)$ and $\sigma : G \to \mathrm{GL}(W)$ be two representations. A *homomorphism*, also known as an *intertwining operator*, is a linear map

$$\varphi : V \to W$$

such that

$$\sigma(g) \circ \varphi = \varphi \circ \rho(g) \quad \text{for all} \quad g \in G.$$

We say that φ is an *isomorphism* if it is bijective.

Definition 1.13. Two matrix representations $\rho_1 : G \to \mathrm{GL}_n(k)$ and $\rho_2 : G \to \mathrm{GL}_n(k)$ are said to be *equivalent* if there exists $A \in \mathrm{GL}_n(k)$ such that

$$\rho_2(g) = A\ \rho_1(g)\ A^{-1} \quad \text{for all} \quad g \in G.$$

If ρ_1 and ρ_2 are two equivalent matrix representations, then the equality of products of matrices $\rho_2(g)A = A\rho_1(g)$ translates to an equality of linear maps

$$\underline{\rho_2(g)} \circ \underline{A} = \underline{A} \circ \underline{\rho_1(g)}$$

in $\mathrm{GL}(k^n)$, which means that the representations $\underline{\rho_1}$ and $\underline{\rho_2}$ of G from Remark 1.10(b) are isomorphic. The converse is also true.

Definition 1.14. Let $\rho : G \to \mathrm{GL}(V)$ be a representation, and let U be a linear subspace of V.

(a) We say that U is *G-stable* if $\rho(g)(u) \in U$ for all $g \in G$ and $u \in U$.

(b) Suppose that U is G-stable. The *subrepresentation of ρ afforded by U* is

$$\rho_U : G \to \mathrm{GL}(U)$$

given by $\rho_U(g)(u) := \rho(g)(u)$ for all $g \in G$ and $w \in U$.

(c) Suppose that U is G-stable. The *quotient representation of ρ afforded by U* is

$$\rho_{V/U} : G \to \mathrm{GL}(V/U)$$

given by $\rho_{V/U}(g)(v+U) := \rho(g)(v) + U$ for all $g \in G$ and $v + U \in V/U$.

The following Lemma is easy to verify directly.

Lemma 1.15. Let $\varphi : V \to W$ be a homomorphism between representations $\rho : G \to \mathrm{GL}(V)$ and $\sigma : G \to \mathrm{GL}(W)$.

(a) $\ker \varphi$ is a G-stable subspace of V.

(b) $\mathrm{Im}\,\varphi$ is a G-stable subspace of W.

(c) There is a natural isomorphism

$$V/\ker\varphi \xrightarrow{\cong} \mathrm{Im}\,\varphi$$

between the G-representations $\rho_{V/\ker\varphi}$ and $\sigma_{\mathrm{Im}\,\varphi}$.

Lemma 1.15(c) is called the *First Isomorphism Theorem* for representations. There are also Second and Third Isomorphism Theorems – see Remark 2.6 below.

Definition 1.16. Let G be a group. The *trivial representation* of G on a vector space V is $\mathbb{1} : G \to \mathrm{GL}(V)$, given by

$$\mathbb{1}(g)(v) = v \quad \text{for all} \quad g \in G, v \in V.$$

Example 1.17. Suppose that k is the finite field $\mathbb{F}_p$ and let $G = \langle g \rangle$ be the cyclic group of order p. Let $\rho : G \to \mathrm{GL}_2(k)$ be the matrix representation given by

$$\rho(g^i) = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \quad \text{for each} \quad i \in \mathbb{Z}.$$

Let $\left\{ v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ be the standard basis for $V = k^2$. Then $U := \langle v_1 \rangle$ is a G-stable subspace, because $\rho(g^i)(v_1) = v_1$ for all i. The subrepresentation $\rho_U : G \to \mathrm{GL}(U)$ and quotient representation $\rho_{V/U} : G \to \mathrm{GL}(V/U)$ in this case are both trivial. However of course ρ itself is not trivial!

Definition 1.18. The representation $\rho : G \to \mathrm{GL}(V)$ is *irreducible* or *simple* if

- V is not the zero vector space, and
- if U is a G-stable subspace of V, then either $U = \{0\}$ or $U = V$.

The irreducible representations are the atoms of representation theory. The major goal of Representation Theory is to find *all* irreducible representations of a given group, up to isomorphism.

Definition 1.19. Let $\rho : G \to \mathrm{GL}(V)$ be a representation and let U be a G-stable subspace. A *G-stable complement* for U in V is a G-stable subspace W such that

$$V = U \oplus W.$$

Recall from Linear Algebra that this means that $U + W = V$ and $U \cap W = \{0\}$.

Example 1.20. Consider the permutation representation of $G = S_3$ afforded by kX, where $X = \{e_1, e_2, e_3\}$ as in Example 1.11. Then

$$U := \langle e_1 + e_2 + e_3 \rangle$$

is a G-stable subspace, with G fixing every vector in U. So, U is a trivial subrepresentation of V. Now let

$$W := \{a_1e_1 + a_2e_2 + a_3e_3 : a_1 + a_2 + a_3 = 0\};$$

this is a G-stable complement to U in V — provided $\mathrm{char}(k) \neq 3$. Let $\mathcal{B} = \{v_1, v_2\}$ where $v_1 := e_1 - e_2$ and $v_2 := e_2 - e_3$ so that $\mathcal{B}$ is a basis for W. Then the degree 2 matrix representation $\sigma := (\rho_W)_{\mathcal{B}} : G \to \mathrm{GL}_2(k)$ afforded by W is determined by

$$\sigma((123)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \sigma((12)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We now come to the first non-trivial result of Representation Theory.

Theorem 1.21 (Maschke)**.** Let G be a finite group and suppose that $|G| \neq 0$ in k. Let U be a G-stable subspace of a finite-dimensional G-representation V. Then U admits at least one G-stable complement W in V.

Proof. By picking a basis for U and extending it to a basis for V we can find some linear complement Z for U in V:

$$V = U \oplus Z.$$

This Z will certainly not be G-stable in general. We will now use an *averaging argument* to replace Z with a G-stable one. To this end, let $\pi : V \to V$ be the *projection map* along the decomposition $V = U \oplus Z$, so that

$$\pi(u+z) = u \quad \text{for all} \quad u \in U, z \in Z.$$

Define a new linear map $\varphi : V \to V$ by the rule

$$\varphi(v) := \frac{1}{|G|}\sum_{x\in G} \rho(x)\pi(\rho(x)^{-1}(v)) \quad \text{for all} \quad v \in V;$$

here, we use the hypothesis that the number $|G|$ is invertible in the field k. We now check directly that φ is a homomorphism of representations. To do this, it is helpful to use the following notation:

$$g \cdot v := \rho(g)(v) \quad \text{for all} \quad g \in G, v \in V.$$

Observe that since ρ is a group homomorphism, this defines a group action of G on the vector space V as in Prelims M1. Fix $g \in G$ and $v \in V$. Then

$$|G|\varphi(g \cdot v) = \sum_{x\in G} x \cdot \pi(x^{-1} \cdot (g \cdot v)).$$

In this finite sum, make the substitution $y^{-1} = x^{-1}g$. As x runs over all elements of G, so does y. Since x is then equal to gy, we obtain

$$|G|\varphi(g \cdot v) = \sum_{y\in G}(gy) \cdot \pi(y^{-1} \cdot v) = g \cdot \sum_{y\in G} y \cdot \pi(y^{-1} \cdot v) = g \cdot |G|\varphi(v).$$

Cancelling $|G|$ we deduce that φ is a homomorphism of representations as claimed. On the other hand, if $u \in U$ then

$$\varphi(u) = \frac{1}{|G|}\sum_{x\in G} x \cdot \pi(x^{-1} \cdot u) = \frac{1}{|G|}\sum_{x\in G} x \cdot (x^{-1} \cdot u) = u$$

because U is G-stable, so $\pi(x^{-1} \cdot u) = x^{-1}u$ for all $x \in G$. So the restriction of φ to U is the identity map. On the other hand, since U is G-stable and since $\pi(V) = U$, the definition of φ shows that $\varphi(V) \subseteq U$. As $\varphi(U) = U$ we actually have $\varphi(V) = U$, so $\operatorname{Im}(\varphi) = U$. Let $W := \ker \varphi$, a G-stable subspace of V by Lemma 1.15(a). Then $\dim W + \dim U = \dim V$ by the Rank-Nullity Theorem, whereas if $v \in W \cap U$ then $0 = \varphi(v) = v$. So, $V = U \oplus W$ and W is a G-stable complement to U in V. □

Remark 1.22. Maschke's Theorem fails if the characteristic of our ground field k happens to divide $|G|$, see Example 1.17.

Definition 1.23. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. We say that ρ is *completely reducible* if there exist G-stable subspaces $U_1, \ldots, U_m$ of V such that

$$V = U_1 \oplus \cdots \oplus U_m$$

and the subrepresentation of G afforded by each U_i is irreducible, *or* if $V = \{0\}$.

Corollary 1.24. Let G be a finite group and suppose that $\mathrm{char}(k) \nmid |G|$. Then every finite dimensional representation $\rho : G \to \mathrm{GL}(V)$ of G is completely reducible.

Proof. Proceed by induction on $\dim V$, the case $\dim V = 0$ being true by definition. Let U_1 be a G-stable non-zero subspace of V of smallest possible dimension. Clearly U_1 is irreducible. Then U_1 admits a G-stable complement W by Maschke's Theorem, Theorem 1.21. Now $\dim W < \dim V$ so by induction, $W = U_2 \oplus \cdots \oplus U_m$ for some G-stable irreducible subspaces $U_2, \cdots, U_m$. Hence $V = U_1 \oplus U_2 \oplus \cdots \oplus U_m$ is also completely reducible. □

2. The group ring

We observed in the proof of Theorem 1.21 that every representation $\rho : G \to \mathrm{GL}(V)$ determines a left action of the group G on V via

$$g \cdot v := \rho(g)(v) \quad \text{for all} \quad g \in G, v \in V.$$

We already noticed that sometimes when working a representation ρ it is cumbersome to keep writing $\rho(g)(v)$ when really one can get away with just $g \cdot v$. On the other hand, since V is a k-vector space it also carries an action of the ground field of scalars k, $(\lambda, v) \mapsto \lambda v$. This may make one suspect that in fact there is a module hiding in the background, and this is in fact the case. Recall the following from Part A Rings and Modules.

Definition 2.1. A *ring* is an abelian group R equipped with an associative multiplication $R \times R \to R$ written $(a, b) \mapsto a \cdot b$, which satisfies the *distributive laws*

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad \text{for all} \quad a, b, c \in R$$

and which admits an identity element $1 \in R$ such that

$$1 \cdot a = a = a \cdot 1 \quad \text{for all} \quad a \in R.$$

In algebraic geometry and algebraic number theory, most rings one encounters are commutative. However in this course rings are most definitely *not* commutative in general!

Definition 2.2. Let G be a finite group. The *group ring* of G (with coefficients in k) is the vector space kG from Definition 1.5, with the following multiplication:

$$\left(\sum_{x \in G} a_x \, x\right) \cdot \left(\sum_{y \in G} b_y \, y\right) = \sum_{g \in G} \left(\sum_{x \in G} a_x b_{x^{-1}g}\right) g.$$

It is easy to check that with this multiplication kG is an associative ring with identity element equal to 1 (the identity element of the group, thought of as a formal linear combination with precisely one non-zero coefficient). The group G becomes embedded into the group ring via $g \mapsto g$: this embedding respects multiplication and thereby realises G as a subgroup of the group of units $kG^\times$ of the ring kG. We will *identify* G with its image in $kG^\times$. In this way, one should think of the ring kG as being an "envelope" of the group G.

Example 2.3. Let $G = \langle x \rangle$ be a cyclic group of order n. Then kG has $G = \{1, x, \cdots, x^{n-1}\}$ as a basis, so it is generated by k and x as a ring, and k commutes with x. Define a ring homomorphism $\varphi : k[T] \to kG$ by setting $\varphi(f(T)) = f(x)$ for each $f(T) \in k[T]$. Then φ is surjective, and $\ker \varphi = \langle T^n - 1 \rangle$. Hence by the First Isomorphism Theorem for Rings,

$$kG \cong k[T]/\langle T^n - 1 \rangle.$$

If in addition the ground field k contains a primitive n-th root of unity ζ, then the polynomial $T^n - 1$ factors into a product of distinct linear factors $(T-1)(T-\zeta)(T-\zeta^2)\cdots(T-\zeta^{n-1})$. Then the Chinese Remainder Theorem implies that

$$kG \cong k[T]/\langle T^n - 1 \rangle \cong \underbrace{k \times k \times \cdots \times k}_{n \text{ times}}.$$

Next, recall the following important definition from Part A Rings and Modules.

Definition 2.4. Let R be a ring. An *R-module* is an abelian group M equipped with a *left R-action* $R \times M \to M$ which satisfies the axioms

$$\begin{aligned} r \cdot (m+n) &= (r \cdot m) + (r \cdot n) \\ (r+s) \cdot m &= (r \cdot m) + (s \cdot m) \\ (r \cdot s) \cdot m &= r \cdot (s \cdot m) \\ 1 \cdot m &= m \end{aligned}$$

for all $r, s \in R, m, n \in M$.

Strictly speaking, what we have defined is at Definition 2.4 is usually called a *left* module. But we will not consider right modules in this course, so all modules we will be concerned with are left modules.

Proposition 2.5. Let V be a vector space and let G be a group.

(a) Suppose that $\rho : G \to \mathrm{GL}(V)$ is a representation. Then V becomes a left kG-module via the action

$$\left(\sum_{x \in G} a_x\, x\right) \cdot v = \sum_{x \in G} a_x \rho(x)(v) \quad \text{for all} \quad a_x \in k, v \in V.$$

(b) Suppose that V is a left kG-module. Then $\rho : G \to \mathrm{GL}(V)$, defined by

$$\rho(g)(v) := g \cdot v \quad \text{for all} \quad g \in G, v \in V$$

is a representation of G.

(c) These recipes set up a bijection between the set of representations $\rho : G \to \mathrm{GL}(V)$ and the set of kG-module structures $kG \times V \to V$ on V.

Important Convention: From now on, we will use the bijective correspondence provided by Proposition 2.5 to freely convert a representation $\rho : G \to \mathrm{GL}(V)$ into the corresponding kG-module V, and vice versa. We will also sometimes say "V is a representation of G" when we actually mean "V is a kG-module".

Remark 2.6. The correspondence between G-representations and kG-modules allows us to apply all general theorems about modules from Part A Rings and Modules to the study of G-representations. For example, the First, Second and Third Isomorphism Theorems, and the Correspondence Theorem hold automatically for G-representations.

Example 2.7. Let A be a ring. The *free A-module of rank* 1 is the abelian group A equipped with the left-multiplication action of A:

$$a \cdot b = ab \quad \text{for all} \quad a, b \in A.$$

A-submodules of this A-module are called *left ideals.*

Definition 2.8. If $A = kG$, the representation $\rho : G \to \mathrm{GL}(kG)$ corresponding to the free kG-module of rank 1 is called the *left regular representation.*

The left regular representation coincides with the permutation representation of G on kG from Definition 1.5 associated with the action of G on $X = G$ by left multiplication.

All of the concepts introduced in §1 above for representations have immediate generalisations in the language of modules. For example, an A-module M is said to be *irreducible*, or *simple*, if M is non-zero, and if whenever N is an A-submodule of M we must have $N = \{0\}$ or $N = M$ itself. A homomorphism of representations is simply a map of kG-modules, also known as a kG-linear map.

Generalising Definition 1.23, we say that an A-module V is *completely reducible* if it is either the zero module, or it is equal to a direct sum of finitely many simple submodules.

Definition 2.9. Let A be a ring. We say that A is *semisimple* if the free A-module of rank 1 is completely reducible.

Maschke's Theorem, Theorem 1.21 gives us the first important example of a semisimple ring.

Example 2.10. Let G be a finite group such that $|G| \neq 0$ in k. Then the group ring kG is semisimple.

Definition 2.11. Let V be an A-module. We say that V is *cyclic* if it can be generated by a single element v: $V = A \cdot v$. The *annihilator* of $v \in V$ is the left ideal

$$\operatorname{ann}_A(v) := \{a \in A : av = 0\}.$$

Clearly every simple module is also cyclic.

Lemma 2.12. Every cyclic A-module V is isomorphic to a quotient module of the free A-module of rank 1: if $V = A \cdot v$ then

$$V \cong A/\operatorname{ann}_A(v).$$

Proof. The map $\varphi : A \to V$ given by $a \mapsto a \cdot v$ is an A-module homomorphism. It is surjective by hypothesis. So by the First Isomorphism Theorem for modules, $V = \operatorname{Im}\varphi \cong A/\ker\varphi$. However $\ker\varphi = \operatorname{ann}_A(v)$. □

The following trivial result has profound consequences.

Lemma 2.13. Let V, W be simple A-modules. Then every non-zero A-linear map $\varphi : V \to W$ is an isomorphism.

Proof. We know that $\ker\varphi$ is an A-submodule of V and that $\operatorname{Im}\varphi$ is an A-submodule of W by the module-theoretic version of Lemma 1.15. Since φ is non-zero, $\ker\varphi$ is not all of V and $\operatorname{Im}\varphi$ is not the zero module. Since V and W are both simple, we conclude that $\ker\varphi$ is zero and $\operatorname{Im}\varphi = W$. Hence φ is bijective, and therefore an isomorphism. □

Proposition 2.14. Let A be a semisimple ring. Then A has only finitely many simple A-modules, up to isomorphism.

Proof. Write $A = V_1 \oplus \cdots \oplus V_r$ for some simple A-submodules V_i of A. Let V be a simple A-module, pick a non-zero vector $v \in V$ and consider the A-module map $\varphi : A \to V$ from Lemma 2.12. Let $\varphi_i : V_i \to V$ be the restriction of φ to V_i, so that if $a = a_1 + \cdots + a_m$ is the decomposition of $a \in A$ with $a_i \in V_i$ for each i, then

$$\varphi(a) = \varphi_1(a_1) + \varphi_2(a_2) + \cdots + \varphi_r(a_r).$$

If φ_i is the zero map for all i, then it follows that φ is also the zero map. So we see that $\varphi_i \neq 0$ for some index i. But now Lemma 2.13 implies that this φ_i must be an isomorphism. So, V is isomorphic to one of the irreducible representations in the list $V_1, V_2, \cdots, V_r$. □

Here is a striking application of our new viewpoint on representations.

Theorem 2.15. Let G be a finite group such that $|G| \neq 0$ in k. Then G has only finitely many irreducible representations, up to isomorphism.

Proof. The ring kG is semisimple by Maschke's Theorem, Theorem 1.21. Now apply Proposition 2.14. □

Definition 2.16. For a finite group G, we will write $r_k(G)$ to denote the number of isomorphism classes of irreducible k-representations of G.

A big motivating question for us will be: how do we compute $r_{\mathbb{C}}(G)$ effectively?

3. Structure of semisimple algebras

We begin with some very general ring theory.

Definition 3.1. The *centre* of the ring A is

$$Z(A) := \{z \in A : az = za \quad \text{for all} \quad a \in A\}.$$

The centre is always a commutative unital subring of A.

Definition 3.2. Let A be a ring and let V be an A-module. The *endomorphism ring* of V, $\operatorname{End}_A(V)$, is the set of all A-module homomorphisms $\varphi : V \to V$, equipped with pointwise addition of homomorphisms, and composition as multiplication.

Note that whenever V is an A-module, it also becomes an $\operatorname{End}_A(V)$-module via $f \cdot v := f(v) \quad \text{for all} \quad f \in \operatorname{End}_A(V)$ and $v \in V$. The two actions (of A and $\operatorname{End}_A(V)$) on V commute pointwise, by definition. This observation shows that the action of any *central* element $z \in Z(A)$ on V is necessarily by an A-module endomorphism.

Definition 3.3. We say that A is a *k-algebra* if it contains k as a central subfield. If, in addition, A is a semisimple ring, we say that A is a *semisimple k-algebra.* A *homomorphism* of k-algebras is a k-linear ring homomorphism.

Theorem 3.4 (Schur's Lemma)**.** Suppose that k is algebraically closed. Let V be a simple module over a finite dimensional k-algebra A. Then every A-module endomorphism of V is given by the action of some scalar $\lambda \in k$, so that

$$\operatorname{End}_A(V) = k1_V.$$

Proof. By Lemma 2.12, V is isomorphic to a quotient module of A, so V is itself finite dimensional as a k-vector space. Let $\varphi : V \to V$ be an A-module endomorphism; then in particular it is a k-linear map so it has at least one eigenvalue $\lambda \in k$ since k is algebraically closed. This means that $\varphi - \lambda 1_V : V \to V$ has a non-zero kernel, and is therefore not an isomorphism. So it must be the zero map, by Lemma 2.13. But then $\varphi = \lambda 1_V$ is the action of $\lambda \in k$, as required. □

Definition 3.5. Let A be a k-algebra and let V be an A-module with $\operatorname{End}_A(V) = k1_V$. Then by Theorem 3.4, every element $z \in Z(A)$ must act on V by a scalar, which we denote by z_V. The ring homomorphism

$$Z(A) \to k, \qquad z \mapsto z_V$$

is called the *central character* of V.

Using these tools, we will now focus on semisimple rings. Recall from Proposition 2.14 that such a ring admits only *finitely many* simple modules up to isomorphism.

Notation 3.6. Until the end of §3, A will denote a fixed semisimple ring, and $V_1, \cdots, V_r$ will denote a complete list of representatives for the isomorphism classes of simple A-modules. We also fix a decomposition

$$A = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} L_{i,j} \tag{3.1}$$

of the A-module A into a direct sum of simple left ideals $L_{i,j}$, where $L_{i,j} \cong V_i$ for each i and j.

We must have $n_1, \cdots, n_r \geq 1$. This is because each V_i occurs as a direct summand of A at least once: this follows from Proposition 2.14. Warning: the left ideals $L_{i,j}$ are *not* unique, in general!

Proposition 3.7. Let A be a finite dimensional semisimple k-algebra and suppose that k is algebraically closed. Then $\dim Z(A) \leqslant r$.

Proof. By Schur's Lemma, Theorem 3.4, we have $\mathrm{End}_A(V_i) = k1_{V_i}$ for all $i = 1, \cdots, r$. So we can define a k-linear map $\psi : Z(A) \to k^r$ by $\psi(z) := (z_{V_1}, z_{V_2}, \cdots, z_{V_r})$. Suppose that $\psi(z) = 0$ for some $z \in Z(A)$; then $z_{V_i} = 0$ for all i; we will show that $z = 0$. Consider the decomposition of $1 \in A$ along the decomposition (3.1):

$$1 = \sum_{i=1}^{r} \sum_{j=1}^{n_i} e_{i,j} \quad \text{for some} \quad e_{i,j} \in L_{i,j}.$$

Then $z = z1 = \sum\limits_{i=1}^{r} \sum\limits_{j=1}^{n_i} ze_{i,j} = \sum\limits_{i=1}^{r} \sum\limits_{j=1}^{n_i} z_{V_i} e_{i,j}$. But $z_{V_i} = 0$ for all i, so $z = 0$. So, ψ is injective and $\dim Z(A) \leqslant \dim k^r = r$. □

Lemma 3.8. Each $B_i := \bigoplus\limits_{j=1}^{n_i} L_{i,j}$ is a two-sided ideal of A, and $A = B_1 \oplus \cdots \oplus B_r$.

Proof. It follows from (3.1) that $A = B_1 \oplus \cdots \oplus B_r$ and that each B_i is a left ideal of A; it will therefore be enough to show that each B_i is also a right ideal in A.

Fix $a \in A$ and consider $L_{i,j} \subseteq B_i$. Let $i' \neq i$ and $1 \leqslant j' \leqslant n_{i'}$ be another pair of indices, and consider the projection $\varphi : A \twoheadrightarrow L_{i',j'}$ along our decomposition (3.1). The restriction of $\varphi \circ r_a : A \to L_{i',j'}$ to $L_{i,j}$ is an A-module homomorphism from $L_{i,j}$ to $L_{i',j'}$. Because $i' \neq i$, these two modules are not isomorphic, so this restriction must be the zero map by Lemma 2.13. Varying i' and j', we see that the projection of $L_{i,j}a$ onto each $B_{i'}$ with $i' \neq i$ is equal to zero. Therefore $L_{i,j}a \subseteq B_i$. But since B_i is equal to the sum of all of the $L_{i,j}$, $B_i a \subseteq B_i$ for all $a \in A$. □

Lemma 3.9. Let R be a k-algebra and suppose that $R = S_1 \oplus \cdots \oplus S_r$ for some non-zero two-sided ideals $S_1, \cdots, S_r$. Then $\dim Z(R) \geq r$.

Proof. Write $1 = e_1 + \cdots + e_r$ for some $e_i \in S_i$. Let $a \in R$ and fix $i = 1, \ldots, r$. Since S_i is a left ideal, $ae_i \in S_i$. Since $a = ae_1 + \cdots + ae_r$, we see that ae_i is the component of a in S_i in the decomposition $R = S_1 \oplus \cdots \oplus S_r$. Similarly since S_i is a right ideal, $e_i a$ is the component of a in S_i in this decomposition. Hence $ae_i = e_i a$ for all i and all $a \in R$, which shows that each e_i is central.

If $i \neq j$ then $e_i e_j \in S_i \cap S_j = \{0\}$ so $e_i e_j = 0$. Hence $e_i = e_i \cdot 1 = e_i \sum\limits_{j=1}^{r} e_j = e_i^2$. We have shown that $\{e_1, \cdots, e_r\}$ forms a set of *pairwise orthogonal idempotents*:

$$e_i e_j = \delta_{i,j} e_i \quad \text{for all} \quad i, j = 1, \cdots, r. \tag{3.2}$$

Now suppose that $\sum\limits_{i=1}^{r} \lambda_i e_i = 0$ for some $\lambda_i \in k$. Multiply this equation by e_j and use (3.2) to get $\lambda_j e_j = 0$. If $e_j = 0$ then for all $a \in S_j$ we have $a = ae_j = 0$, contradicting the assumption that $S_j \neq \{0\}$. So $e_j \neq 0$ for all $j = 1, \ldots, r$, and this shows that $\{e_1, \cdots, e_r\}$ is linearly independent over k. Hence $r \leqslant \dim Z(R)$. □

Theorem 3.10. Let A be a finite dimensional semisimple k-algebra and suppose that k is algebraically closed. Then $r = \dim Z(A)$.

Proof. By Proposition 3.7 we have $r \geq \dim Z(A)$. By Lemma 3.8 we have $A = B_1 \oplus \cdots \oplus B_r$ for some two-sided ideals B_r, so Lemma 3.9 gives the reverse inequality $r \leqslant \dim Z(A)$. □

We have now related the number of isomorphism classes of simple modules over our semisimple k-algebra to the centre of A, which motivates the question of calculating $\dim Z(kG)$. Computing the centre of group rings is very easy.

Definition 3.11. For a finite group G, let $s(G)$ denote the number of conjugacy classes of G.

Proposition 3.12. Let G be a finite group and let $C_1, \cdots, C_s$ be the conjugacy classes of G. For each $i = 1, \ldots, s$, define the *conjugacy class sum* of C_i to be

$$\widehat{C_i} := \sum_{x \in C_i} x \in kG.$$

Then $\{\widehat{C_1}, \cdots, \widehat{C_s}\}$ is a basis for $Z(kG)$ as a vector space, so

$$\dim Z(kG) = s(G).$$

Proof. Problem Sheet 1. □

Corollary 3.13. Let G be a finite group, and let k be an algebraically closed field with $|G| \neq 0$ in k. Then $r_k(G) = s(G)$.

Proof. By Theorem 1.21, kG is a semisimple k-algebra with $\dim Z(kG) = s(G)$ by Proposition 3.12. Now apply Theorem 3.10. □

We were able to obtain this striking result without really understanding the internal structure of the ring kG properly. With a little additional effort, this structure will become completely transparent at least in the case where the ground field k is algebraically closed and where Maschke's Theorem applies.

We continue with the notation established at (3.6) above.

Lemma 3.14.

(a) Each B_i is a ring with identity element e_i.
(b) A is isomorphic to the *product* of the rings (B_i, e_i):

$$A \cong B_1 \times \cdots \times B_r.$$

(c) Each B_i is itself a semisimple ring, with unique simple module V_i.

Proof. (a) Lemma 3.8 implies that B_i is an additive subgroup of A, stable under multiplication. We saw in the proof of Lemma 3.9 that for any $a \in A$, $ae_i = e_i a$ is the B_i-component of a along the decomposition $A = B_1 \oplus \cdots \oplus B_r$. So $ae_i = e_i a = a$ for all $a \in B_i$ which says that e_i is an identity element in B_i.

(b) The isomorphism sends $a \in A$ to $(ae_1, \cdots, ae_r) \in B_1 \times \cdots \times B_r$.

(c) Fix $\ell = 1, \ldots, n_i$ and suppose that U is a B_i-submodule of $L_{i,\ell}$. Then

$$A \cdot U = \left(\bigoplus_{j=1}^{r} B_j \right) \cdot U \leqslant U$$

because by (3.2), $B_j \cdot U \leqslant B_j \cdot B_i = B_j e_j \cdot e_i B_i = 0$ if $j \neq i$, and $B_i \cdot U \leqslant U$ as U is a B_i-submodule. Hence U is also an A-submodule of $L_{i,\ell}$, so U is either zero or all of $L_{i,\ell}$ because $L_{i,\ell}$ is a simple A-module. We've shown that $L_{i,\ell}$, and hence also V_i, are simple B_i-modules.

Since $B_i = \bigoplus_{j=1}^{n_i} L_{i,j}$, it is a semisimple ring. The proof of Proposition 2.14 now shows that V_i is the *only* simple B_i-module, up to isomorphism. □

Warning: even though each B_i is an additive subgroup of A stable under multiplication, *it is not a unital subring* when $r \geq 2$, because its identity element e_i is then not equal to the identity element 1 in A.

Definition 3.15. Let A be a ring. The *opposite ring* to A, A^{op}, has A as the underlying abelian group, but with the following new multiplication:

$$a \star b := ba \quad \text{for all} \quad a, b \in A^{\text{op}}.$$

Proposition 3.16. Let B be a semisimple ring with exactly one simple module V, up to isomorphism. Suppose that $B \cong \overbrace{V \oplus \cdots \oplus V}^{n \text{ times}}$ as a left B-module, and let $D := \operatorname{End}_B(V)$. Then there is a ring isomorphism

$$B \cong M_n(D^{\text{op}}).$$

Proof. By Problem Sheet 2, we know that B is isomorphic to $\mathrm{End}_B(B)^{\mathrm{op}}$. Since $B = V^n$ as a left B-module, we have $\mathrm{End}_B(B) \cong M_n(D)$. Hence, $B \cong \mathrm{End}_B(B)^{\mathrm{op}} \cong M_n(D)^{\mathrm{op}} \cong M_n(D^{\mathrm{op}})$. See By Problem Sheet 2 for more details. □

Theorem 3.17 (Artin-Weddernburn)**.** Suppose that k is an algebraically closed field and that A is a finite dimensional semisimple k-algebra. Then there exist positive integers $n_1, n_2, \cdots, n_r$ and a k-algebra isomorphism

$$A \quad \overset{\cong}{\longrightarrow} \quad M_{n_1}(k) \times \cdots \times M_{n_r}(k).$$

Proof. By Lemma 3.14, we may assume that $r = 1$, so that A has exactly one simple module V up to isomorphism. Then $A \cong M_n(D^{\mathrm{op}})$ where $D := \mathrm{End}_A(V)$, by Lemma 3.16. But $D \cong k$ by Schur's Lemma, Theorem 3.4. □

Corollary 3.18. Suppose that k is algebraically closed. Let G be a finite group such that $|G| \neq 0$ in k and let $V_1, \cdots, V_r$ be a complete list of pairwise non-isomorphic simple kG-modules.
(a) $kG \cong V_1^{\dim V_1} \oplus V_2^{\dim V_2} \oplus \cdots \oplus V_r^{\dim V_r}$ as a kG-module.
(b) $|G| = \sum_{i=1}^{r} (\dim V_i)^2$.

Proof. (a) kG is a semisimple ring by Maschke's Theorem, Theorem 1.21, so $kG \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ by the Artin-Wedderburn Theorem, Theorem 3.17. The matrix algebra $M_n(k)$ acts on the space of column vectors k^n naturally by left multiplication, k^n is then a simple $M_n(k)$-module and $M_n(k)$ is isomorphic to a direct sum of precisely n copies of this simple module by Problem Sheet 1. So, $n_i = \dim V_i$ for each $i = 1, \dots, r$.

(b) This is immediate from part (a). □

4. Multilinear algebra

The regular representation of G afforded by kG gives a good way to theoretically bound the number of possible irreducible representations. But it does not really help us to find them. We harness the full power of linear algebra here to find many new representations from old. Throughout §4, G will denote a fixed finite group. The following observation will be useful for constructing G-representations.

Lemma 4.1. Let V be a vector space and let $G \times V \to V$ be a G-action on the set V. Then this extends to a kG-module structure on V if and only if the G-action on V is *linear*, which means that the following condition holds:

$$g \cdot (v + \lambda w) = (g \cdot v) + \lambda(g \cdot w) \quad \text{for all} \quad g \in G, v, w \in V, \lambda \in k.$$

Definition 4.2. Let V, W be G-representations. The *(external) direct sum* is the vector space

$$V \oplus W := V \times W$$

which is again a G-representation via

$$g \cdot (v, w) = (g \cdot v, g \cdot w) \quad \text{for all} \quad g \in G, v \in V, w \in W.$$

We will usually identify V and W with their images $\{(v, 0) : v \in V\}$ and $\{(0, w) : w \in W\}$ inside $V \times W$, respectively. The sum of these images is all of $V \times W$ and their intersection is $\{(0, 0)\}$, so this notation $V \oplus W$ is consistent with the one you've met in Linear Algebra.

Definition 4.3. Let V be a G-representation. The *dual representation* is the space V^* of all linear functions $f : V \to k$ on V. The group G acts on V^* via

$$(g \cdot f)(v) := f(g^{-1} \cdot v) \quad \text{for all} \quad g \in G, f \in V^*, v \in V.$$

This action is linear so we get a new G-representation V^* of the same dimension as V. Note the inverse appearing in this definition! Without it, the axiom $g \cdot (h \cdot f) = (gh) \cdot f$ for a G-action does not hold.

Definition 4.4. Let V, W be G-representations. The vector space $\operatorname{Hom}(V, W)$ of all linear maps from V to W admits a linear G-action given by

$$(g \cdot f)(v) = g \cdot f(g^{-1} \cdot v) \quad \text{for all} \quad g \in G, f \in \operatorname{Hom}(V, W), v \in V.$$

In the case where W is the trivial 1-dimensional representation, we recover the dual space $\operatorname{Hom}(V, k) = V^*$, so Definition 4.4 is a generalisation of Definition 4.3.

Lemma 4.5. Let V be a finite dimensional G-representation. The natural biduality isomorphism from Part A Linear Algebra

$$\tau : V \to (V^*)^*, \quad \tau(v)(f) := f(v) \quad \text{for all} \quad f \in V^*, v \in V$$

is an isomorphism of G-representations.

Definition 4.6. Let V and W be two vector spaces, let $\{v_1, \cdots, v_m\}$ be a basis for V and let $\{w_1, \cdots, w_n\}$ be a basis for W. The *tensor product* of V and W,

$$V \otimes W,$$

is the free vector space (see Definition 1.4) on the set of formal symbols

$$\{v_i \otimes w_j : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}.$$

If $v = \sum_{i=1}^{m} \lambda_i v_i$ and $w = \sum_{j=1}^{n} \mu_j w_j$ are elements of V and W respectively, we define the *elementary tensor*

$$v \otimes w := \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_i \mu_j (v_i \otimes w_j) \in V \otimes W \tag{4.1}$$

Remarks 4.7.

(a) From the definition we see that $\dim V \otimes W = (\dim V)(\dim W)$.
(b) The elementary tensors span $V \otimes W$.
(c) Not every element of $V \otimes W$ is an elementary tensor $v \otimes w$.

It may appear that this definition depends on the choice of bases for V and W. To address this, we have the following

Lemma 4.8. Let $\{v'_1, \cdots, v'_m\}$ and $\{w'_1, \cdots, w'_n\}$ be other bases for V and W, respectively. Then

$$X' := \{v'_i \otimes w'_j : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$$

is a basis for $V \otimes W$.

Proof. The elementary tensors in $V \otimes W$ distribute, in the sense that

$$(v+v')\otimes(w+w') = (v\otimes w)+(v\otimes w')+(v'\otimes w)+(v'\otimes w') \quad \text{for all} \quad v, v' \in V, w, w' \in W$$

and also that $(\lambda v) \otimes w = \lambda(v \otimes w) = v \otimes (\lambda w)$ for all $v \in V, w \in W, \lambda \in k$.

Using this observation, we can now write each v_i as a linear combination of $\{v'_1, \cdots, v'_m\}$ and each w_j as a linear combination of $\{w'_1, \cdots, w'_n\}$, and see that the original basis vectors $v_i \otimes w_j$ for $V \otimes W$ all lie in the span of X'. Therefore X' spans $V \otimes W$ as a vector space, but being a set of size at most mn, it must be linearly independent and is therefore a basis. □

Note that there is a canonical map

$$\otimes : V \times W \to V \otimes W, \quad (v, w) \mapsto v \otimes w$$

which is *bilinear*, in the sense that for all $\lambda, \mu \in k, v_1, v_2 \in V, w_1, w_2 \in W$ we have

$$(\lambda v_1 + v_2) \otimes (\mu w_1 + w_2) = \lambda\mu(v_1 \otimes w_1) + \lambda(v_1 \otimes w_2) + \mu(v_2 \otimes w_1) + (v_2 \otimes w_2).$$

In fact, this map is *universal* with respect to this property, in the following sense.

Lemma 4.9 (Universal Property of Tensor Product)**.** Let V and W be vector spaces. Then for every bilinear map $b : V \times W \to U$ to some third vector space U, there is a unique linear map $\widetilde{b} : V \otimes W \to U$ such that

$$b(v, w) = \widetilde{b}(v \otimes w) \quad \text{for all} \quad v, w \in V.$$

Proof. Fix bases $\{v_1, \cdots, v_n\}$ for V and $\{w_1, \cdots, w_m\}$ for W. Let $b : V \times W \to U$ be a bilinear map, and define $\tilde{b} : V \otimes W \to U$ to be the unique linear map which sends the basis vector $v_i \otimes w_j \in V \otimes W$ to $b(v_i, w_j)$. Let $v = \sum_i \lambda_i v_i \in V$ and $w = \sum_j \mu_j w_j \in W$. Then $\tilde{b}$ sends the elementary tensor $v \otimes w = \sum\limits_{i,j} \lambda_i \mu_j v_i \otimes w_j$ to

$$\sum_{i,j} \lambda_i \mu_j b(v_i, w_j) = b\left(\sum_i \lambda_i v_i, \sum_j \mu_j w_j\right) = b(v, w)$$

because b is bilinear. So this linear map $\widetilde{b} : V \otimes W \to U$ satisfies the required property. If $c : V \otimes W \to U$ is another linear map such that $b(v, w) = c(v \otimes w)$ for all $v \in V, w \in W$, then $c(v_i \otimes w_j) = b(v_i, w_j) = \widetilde{b}(v_i \otimes w_j)$ shows that c agrees with $\widetilde{b}$ on a basis for $V \otimes W$, so $c = \widetilde{b}$. □

Definition 4.10. Let V and W be finite dimensional kG-modules. Define a G-action on the tensor product $V \otimes W$ by setting

$$g \cdot (v \otimes w) := (g \cdot v) \otimes (g \cdot w) \quad \text{for all} \quad g \in G, v \in V, w \in W.$$

This defines the *tensor product representation* $V \otimes W$.

It is straightforward to check that this defines a linear G-action on $V \otimes W$ in the sense of Lemma 4.1, and therefore a G-representation.

Lemma 4.11. Let V and W be finite dimensional kG-modules. Then there is an isomorphism of kG-modules

$$V^* \otimes W \xrightarrow{\cong} \operatorname{Hom}(V, W).$$

Proof. For every $f \in V^*$ and $w \in W$, we have a linear map $b(f, w) : V \to W$ given by $b(f, w)(v) := f(v)w$. The resulting map $b : V^* \times W \to \operatorname{Hom}(V, W)$ is bilinear, so by Lemma 4.9 it extends to a linear map

$$\alpha : V^* \otimes W \to \operatorname{Hom}(V, W)$$

given by $\alpha(f \otimes w)(v) := f(v)w$ for all $f \in V^*, w \in W, v \in V$. Let $\{v_1, \cdots, v_n\}$ be a basis for V and let $\{v_1^*, \cdots, v_n^*\}$ be the corresponding dual basis for V^*. Then we define a linear map

$$\beta : \operatorname{Hom}(V, W) \to V^* \otimes W, \quad f \mapsto \sum_{i=1}^{n} v_i^* \otimes f(v_i).$$

Let $f \in \operatorname{Hom}(V, W)$ and $v \in V$; then

$$\begin{aligned}(\alpha \circ \beta)(f)(v) &= \alpha(\beta(f))(v) = \sum_{i=1}^{n} \alpha(v_i^* \otimes f(v_i))(v) = \sum_{i=1}^{n} v_i^*(v) f(v_i) \\ &= f\left(\sum_{i=1}^{n} v_i^*(v) v_i\right) = f(v)\end{aligned}$$

which shows that $\alpha \circ \beta = 1_{\operatorname{Hom}(V,W)}$. We leave the verification that $\beta \circ \alpha = 1_{V^* \otimes W}$ and that α is a homomorphism of kG-modules to Problem Sheet 2. □

It turns out that the tensor square $V \otimes V$ is reducible whenever $\dim V \geq 2$.

Definition 4.12. Suppose that $\operatorname{char}(k) \neq 2$ and let V be a finite dimensional vector space.

(a) For each $v, w \in V$, define

$$vw := \frac{1}{2}(v \otimes w + w \otimes v) \in V \otimes V.$$

The *symmetric square* of V is the following subspace of $V \otimes V$:

$$S^2 V := \langle \{vw : v, w \in V\} \rangle.$$

(b) For each $v, w \in V$, define

$$v \wedge w := \frac{1}{2}(v \otimes w - w \otimes v) \in V \otimes V.$$

The *alternating square* of V is the following subspace of $V \otimes V$:

$$\bigwedge^2 V := \langle \{v \wedge w : v, w \in V\} \rangle.$$

Note that $vw = wv$ in S^2V and that $v \wedge w = -w \wedge v$ in $\bigwedge^2 V$ for all $v, w \in V$.

Lemma 4.13. Let $\dim V = n$ and suppose that $\operatorname{char}(k) \neq 2$.

(a) $V \otimes V = S^2 V \oplus \bigwedge^2 V$.

(b) $\dim S^2 V = \frac{n(n+1)}{2}$ and $\dim \bigwedge^2 V = \frac{n(n-1)}{2}$.

(c) If V is a G-representation, then so are S^2V and $\bigwedge^2 V$ via

$$g \cdot (vw) = (g \cdot v)(g \cdot w) \quad \text{and} \quad g \cdot (v \wedge w) = (g \cdot v) \wedge (g \cdot w)$$

for all $g \in G, v, w \in V$.

Proof. (a) Let $S_2 := \langle \sigma \rangle$ be the cyclic group of order 2. Since $\operatorname{char}(k) \neq 2$, the group ring kS_2 admits orthogonal idempotents $e_1 := \frac{1+\sigma}{2} \in kS_2$ and $e_2 := \frac{1-\sigma}{2} \in kS_2$, which give rise to the ideal decomposition from Lemma 3.8

$$kS_2 = kS_2 e_1 \oplus kS_2 e_2 = ke_1 \oplus ke_2.$$

It follows that every kS_2-module M admits an even-odd decomposition

$$M = e_1 M \oplus e_2 M = \{m \in M : \sigma m = m\} \oplus \{m \in M : \sigma m = -m\}.$$

Now S_2 acts linearly on $V \otimes V$ as follows:

$$\sigma \cdot (v \otimes w) = w \otimes v \quad \text{for all} \quad v, w \in V.$$

Then $S^2V = e_1 \cdot (V \otimes V)$ is the even part of $V \otimes V$ and $\bigwedge^2 V = e_2 \cdot (V \otimes V)$ is the odd part of $V \otimes V$. The even-odd decomposition then implies $V \otimes V = S^2V \oplus \bigwedge^2 V$.

(b) If $\{v_1, \ldots, v_n\}$ is a basis for V then $\{v_i \otimes v_j : 1 \leqslant i, j \leqslant n\}$ spans $V \otimes V$, so $\{e_1 \cdot (v_i \otimes v_j) : 1 \leqslant i, j \leqslant n\}$ spans $S^2V = e_1 \cdot (V \otimes V)$. Now $e_1 \cdot (v_i \otimes v_j) = v_i v_j = v_j v_i$, so already $\{v_i v_j : 1 \leqslant i \leqslant j \leqslant n\}$ spans S^2V, and therefore

$$\dim S^2V \leqslant \frac{n(n+1)}{2}.$$

Similarly, $\{e_2 \cdot (v_i \otimes v_j) = v_i \wedge v_j : 1 \leqslant i < j \leqslant n\}$ spans $\bigwedge^2 V$, and therefore

$$\dim \bigwedge^2 V \leqslant \frac{n(n-1)}{2}.$$

But $\dim V \otimes V = n^2$, so $V \otimes V = S^2V \oplus \bigwedge^2 V$ implies the result.

(c) We have two groups acting on $V \otimes V$, namely G and S_2. Now

$$\sigma \cdot (g \cdot (v \otimes w)) = \sigma(g \cdot v \otimes g \cdot w) = g \cdot w \otimes g \cdot v = g \cdot (w \otimes v) = g \cdot (\sigma \cdot (v \otimes w))$$

for any $v, w \in V$ and $g \in G$. This means that these two actions *commute pointwise.* In particular, the G-action preserves $S^2V = e_1 \cdot (V \otimes V)$ and $\bigwedge^2 V = e_2 \cdot (V \otimes V)$. Hence S^2V and $\bigwedge^2 V$ inherit a linear G-action from $V \otimes V$ as claimed. □

Using similar ideas, it is possible to find proper kG-submodules of the tensor cube $V \otimes V \otimes V$, one for each irreducible representation of kS_3. Similarly we obtain a decomposition of the nth tensor power $V^{\otimes n}$ of V as a direct sum of kG-submodules $S^\lambda(V)$, one for each irreducible representation λ of the symmetric group S_n. This construction $V \mapsto S^\lambda(V)$ is called a *Schur functor.*

5. Character theory

We will now specialise to the case $k = \mathbb{C}$. It turns out that G-representations are determined by what appears to be very little information at all, namely the knowledge of the *character* of that representation.

Definition 5.1. Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation of G. The *character* of ρ is the function

$$\chi_\rho : G \to \mathbb{C}, \quad g \mapsto \operatorname{tr} \rho(g).$$

The *degree* of a character χ_ρ is the degree of the representation ρ.

We will also write χ_V to denote the character of the representation afforded by a $\mathbb{C}G$-module V, when the $\mathbb{C}G$-module structure on V is understood. This notion only depends on the isomorphism class of the $\mathbb{C}G$-module V, and the isomorphism class of the representation ρ.

Definition 5.2. A function $f : G \to \mathbb{C}$ is said to be a *class function* if it is constant on conjugacy classes of G:

$$f(xgx^{-1}) = f(g) \quad \text{for all} \quad g, x \in G.$$

We will denote the space of all class functions on G by $\mathcal{C}(G)$.

Lemma 5.3. The character χ_V of any finite dimensional kG-module V is a class function.

Proof. If $\rho : G \to \mathrm{GL}(V)$ is the corresponding representation, then the linear endomorphism $\rho(g)$ of V is conjugate to $\rho(xgx^{-1})$ in $\mathrm{GL}(V)$. But conjugate linear maps have the same trace: $\mathrm{tr}(ABA^{-1}) = \mathrm{tr}((AB)A^{-1}) = \mathrm{tr}(A^{-1}(AB)) = \mathrm{tr}(B)$ for any $A, B \in \mathrm{GL}(V)$. □

Definition 5.4. Let G be a finite group, let $\{g_1, \cdots, g_s\}$ be a set of representatives for the conjugacy classes of G and let $V_1, \cdots, V_r$ be a complete list of representatives for the isomorphism classes of simple $\mathbb{C}G$-modules. The *character table* of G is the $r \times s$ array with (i, j)-th entry being given by $\chi_{V_i}(g_j)$.

Recall from Corollary 3.13 that in fact $r = r_{\mathbb{C}}(G)$ is equal to $s = s(G)$, so the character table is always square. If a representation ρ is known, computing its character is usually straightforward.

We record some basic facts about characters.

Lemma 5.5. Let $\rho : G \to \mathrm{GL}(V)$ be a finite dimensional representation.

(a) $\chi_V(1) = \dim V$.
(b) $\chi_V(g) = \chi_V(1)$ if and only if $\rho(g) = 1$.
(c) If $\dim V = 1$ then χ is a group homomorphism.
(d) If G is abelian and V is irreducible, then $\dim V = 1$.

Proof. Problem Sheet 3. □

Example 5.6.

(a) The character table of the cyclic group of order 3, $G = \{1, x, x^2\}$ is

	1	x	x^2
$\mathbb{1}$	1	1	1
χ	1	ω	ω^2
χ^2	1	ω^2	ω

where $\omega := e^{\frac{2\pi i}{3}}$ is a primitive cube root of unity.

(b) Let $G = S_3$. In addition to the trivial character, we have the sign character $\epsilon : S_3 \to \{\pm 1\} \subset \mathbb{C}^\times$, defined by

$$\epsilon(\sigma) = \begin{cases} 1 & \text{if} \quad \sigma \quad \text{is even,} \\ -1 & \text{if} \quad \sigma \quad \text{is odd.} \end{cases}$$

We also have the two-dimensional irreducible representation W of S_3 from Example 1.20. Since $1^2 + 1^2 + 2^2 = 6 = |S_3|$, we have found all the characters, and the character table of S_3 is

	1	(123)	(12)
$\mathbb{1}$	1	1	1
ϵ	1	1	-1
χ_W	2	-1	0

Characters of degree 1 are called *linear characters*. We have the following important consequence of our study of the group ring $\mathbb{C}G$ from §3.

Proposition 5.7. Let $\chi_1, \cdots, \chi_r$ be the complete list of characters of the irreducible complex representations of the finite group G. Then

$$\chi_1(1)^2 + \cdots + \chi_r(1)^2 = |G|$$

Proof. Suppose that the simple kG-module V_i affords the character χ_i. Then $\chi_i(1) = \dim V_i$ by Lemma 5.5(a); now use Corollary 3.18(b). □

Definition 5.8. Let N be a normal subgroup of the finite group G and let $\rho : G/N \to \mathrm{GL}(V)$ be a representation. The *inflated representation* of G

$$\dot{\rho} : G \to \mathrm{GL}(V)$$

is defined by $\dot{\rho}(g) := \rho(gN)$ for all $g \in G$.

Definition 5.9. Let G be a finite group. The *derived subgroup*, G', is the subgroup of G generated by all *commutators* $[x, y] := xyx^{-1}y^{-1}$ in G:

$$G' := \langle xyx^{-1}y^{-1} : x, y \in G \rangle.$$

Lemma 5.10. Let G be a finite group. Then G has precisely $|G : G'|$ distinct complex linear characters.

Proof. Problem Sheet 3. □

Example 5.11. Let $G = A_4$ be the alternating group of order 12. We know that A_4 has a normal subgroup of order 4, called the *Klein four-group*

$$V_4 := \{1, (12)(34), (14)(23), (13)(24)\}.$$

Since A_4/V_4 has order 3, it must be a cyclic group of order 3, hence abelian, so $A_4' \leqslant V_4$ and $|A_4'| \in \{1, 2, 4\}$. No subgroup of order 2 in V_4 is normal in A_4. So, A_4' has to be V_4: it cannot be the trivial group since A_4 is non-abelian.

Conclusion: A_4 admits 3 distinct linear characters, inflated from $A_4/V_4 \cong C_3$.

Definition 5.12. Let G be a finite group. The *inner product on class functions*

$$\langle -, - \rangle : \mathcal{C}(G) \times \mathcal{C}(G) \to \mathbb{C}$$

is defined as follows:

$$\langle \varphi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g)$$

It is routine to verify that this is indeed a complex inner product on $\mathcal{C}(G)$, which means that the following properties are satisfied for all $\varphi, \psi \in \mathcal{C}(G)$ and $\lambda \in \mathbb{C}$:

- $\langle \lambda\varphi, \psi\rangle = \overline{\lambda}\langle \varphi, \psi\rangle$ and $\langle \varphi, \lambda\psi\rangle = \lambda\langle \varphi, \psi\rangle$
- $\langle -, -\rangle$ is additive in both variables,
- $\langle \varphi, \psi\rangle = \overline{\langle \psi, \varphi\rangle}$,
- $\langle \varphi, \varphi\rangle \geq 0$ with equality if and only if $\varphi = 0$.

We can now state our next big theorem.

Theorem 5.13 (Row Orthogonality)**.** Let φ, ψ be irreducible characters of the finite group G. Then

$$\langle \varphi, \psi\rangle = \begin{cases} 1 & \text{if} \quad \varphi = \psi \\ 0 & \text{if} \quad \varphi \neq \psi. \end{cases}$$

Theorem 5.13 has the following striking consequence.

Corollary 5.14. Let V and W be two finite dimensional kG-modules. Then V is isomorphic to W if and only if $\chi_V = \chi_W$.

Proof. Let $\chi_1, \cdots, \chi_r$ be the complete list of characters of the irreducible complex representations of G, and suppose that V_i is the simple kG-module with character χ_i. By Maschke's Theorem, Theorem 1.21, we know that V is a direct sum of simple kG-modules. Since $V_1, \cdots, V_r$ are the *only* possible simple kG-modules (up to isomorphism) we can find non-negative integers $a_1, \cdots, a_r$ such that

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}.$$

We say that a_i is the *multiplicity* of V_i in V. Passing to characters, we have

$$\chi_V = a_1\chi_1 + \cdots + a_r\chi_r$$

and now Theorem 5.13 tells us that we can recover a_i from χ_V as follows:

$$\langle \chi_i, \chi_V\rangle = \langle \chi_i, \sum_{j=1}^{r} a_j\chi_j\rangle = \sum_{j=1}^{r} a_j\delta_{i,j} = a_i.$$

Now, if $\chi_V = \chi_W$ and $W \cong V_1^{b_1} \oplus \cdots \oplus V_r^{b_r}$ as a kG-module, then for each $i = 1, \ldots, r$, $a_i = \langle \chi_i, \chi_V\rangle = \langle \chi_i, \chi_W\rangle = b_i$. Therefore $V \cong V_1^{a_1} \oplus \cdots \oplus V_r^{a_r} = V_1^{b_1} \oplus \cdots V_r^{b_r} = W$ and hence $V \cong W$. The converse implication is trivial. □

Here is an another consequence of Theorem 5.13.

Corollary 5.15. The irreducible characters of G form an orthonormal basis for $\mathcal{C}(G)$.

Proof. We know that $\langle \chi_i, \chi_j\rangle = \delta_{i,j}$ by Theorem 5.13, so the χ_i's are pairwise orthogonal elements of the inner product space $\mathcal{C}(G)$ by Lemma 5.3. Now $\dim \mathcal{C}(G) = s(G) = r_{\mathbb{C}}(G) = r$ by Corollary 3.13, so $\{\chi_1, \cdots, \chi_r\}$ forms a basis for $\mathcal{C}(G)$. □

Let us see how to use Theorem 5.13 to compute character tables: we can complete the analysis that we started in Example 5.11 above, but first, some notation.

Definition 5.16. Let G be a finite group and let $g \in G$.

(a) g^G denotes the *conjugacy class* of g in G:

$$g^G := \{g^x : x \in G\} \quad \text{where} \quad g^x := x^{-1}gx.$$

(b) $C_G(g)$ denotes the *centraliser* of g in G:

$$C_G(g) = \{x \in G : gx = xg\}.$$

Lemma 5.17. For any $g \in G$ we have $|g^G| \cdot |C_G(g)| = |G|$.

Proof. Apply the Orbit-Stabiliser Theorem from Prelims M1 to the conjugation action of G on itself: the orbit of $g \in G$ is its conjugacy class, and the stabiliser of g is precisely the centraliser $C_G(g)$. □

Example 5.18. Let $G = A_4$. Then $A_4' = V_4$ and G has 3 distinct linear characters by Example 5.11. The representatives for the conjugacy classes in A_4 are 1, $g_2 := (12)(34)$, $g_3 := (123)$ and $g_4 := (132)$. So, A_4 has exactly 4 conjugacy classes, and therefore $r_{\mathbb{C}}(G) = s(G) = 4$ because the character table is square by Corollary 3.13. So, the character table of A_4 looks as follows:

g	1	g_2	g_3	g_4
$\lvert g^G\rvert$	1	3	4	4
$\lvert C_G(g)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	d	a	b	c

where $\omega = e^{\frac{2\pi i}{3}}$. Proposition 5.7 tells us that $1^2 + 1^2 + 1^2 + d^2 = |G| = 12$. Then Lemma 5.5(a) implies that $d = 3$ is the only possibility. Now, by Theorem 5.13:

$$0 = |G|\langle \chi_1, \chi_4\rangle = 1 \cdot 1 \cdot 3 + |g_2^G| \cdot 1 \cdot a + |g_3^G| \cdot 1 \cdot b + |g_4^G| \cdot 1 \cdot c = 3 + 3a + 4b + 4c$$

and

$$0 = |G|\langle \chi_2, \chi_4\rangle = 1 \cdot 1 \cdot 3 + |g_2^G| \cdot 1 \cdot a + |g_3^G| \cdot \omega \cdot b + |g_4^G| \cdot \omega^2 \cdot c = 3 + 3a + 4\omega b + 4c\omega^2$$

and

$$0 = |G|\langle \chi_3, \chi_4\rangle = 1 \cdot 1 \cdot 3 + |g_2^G| \cdot 1 \cdot a + |g_3^G| \cdot \omega^2 \cdot b + |g_4^G| \cdot \omega \cdot c = 3 + 3a + 4\omega^2 b + 4c\omega.$$

Solving these linear equations we see that $a = -1$ and $b = c = 0$. So, the full character table of A_4 is

g	1	g_2	g_3	g_4
$\lvert g^G\rvert$	1	3	4	4
$\lvert C_G(g)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	$0.$

We now start working towards the proof of Theorem 5.13.

Definition 5.19. Let V be a $\mathbb{C}G$-module. The *invariant submodule* of V is

$$V^G := \{v \in V : g \cdot v = v \quad \text{for all} \quad g \in G\}.$$

Clearly V^G is the largest subspace of V on which G acts trivially. How do we calculate the dimension of V^G? Using a special case of Theorem 5.13:

Proposition 5.20 (Fixed Point Formula)**.** Let G be a finite group and let V be a finite dimensional $\mathbb{C}G$-module. Then

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) = \langle \mathbb{1}, \chi_V \rangle.$$

Proof. Let $e := \frac{1}{|G|} \sum\limits_{g \in G} g \in \mathbb{C}G$. Then $ge = eg = e$ for all $g \in G$ so $e^2 = e$; this is why e is called the *principal idempotent* of $\mathbb{C}G$. We have

$$V = e \cdot V \oplus (1 - e) \cdot V.$$

Now if $g \in G$ then $g \cdot (e \cdot v) = (ge) \cdot v = e \cdot v$ so $e \cdot V \leqslant V^G$; on the other hand if $v \in V^G$ then $g \cdot v = v$ for all $g \in G$, so $|G| e \cdot v = \sum\limits_{g \in G} g \cdot v = |G| v$ whence $v = e \cdot v$ and $v \in e \cdot V$. We have shown that

$$e \cdot V = V^G.$$

The action of $e \in \mathbb{C}G$ on V is a linear map $e_V : V \to V$ which is an idempotent with image $e \cdot V$. So, writing $\rho : G \to \mathrm{GL}(V)$ for the representation afforded by V,

$$\dim V^G = \dim e \cdot V = \mathrm{tr}(e_V) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\, \rho(g) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g). \qquad \square$$

Before we give the proof of Theorem 5.13, we need to compute the characters of the representations obtained through various multilinear constructions from §4. Observe that the vector space of class functions $\mathcal{C}(G)$ is in fact a *commutative ring*, via pointwise multiplication of functions:

$$(\varphi\psi)(g) := \varphi(g)\psi(g) \quad \text{for all} \quad g \in G.$$

Proposition 5.21. Let G be a finite group and let V, W be finite dimensional $\mathbb{C}G$-modules. Then we have the following equalities in $\mathcal{C}(G)$:

(a) $\chi_{V^*} = \overline{\chi_V}$,
(b) $\chi_{V \oplus W} = \chi_V + \chi_W$,
(c) $\chi_{V \otimes W} = \chi_V \chi_W$,
(d) $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\chi_W$,
(e) $\chi_{S^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2))$ for all $g \in G$,
(f) $\chi_{\bigwedge^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2))$ for all $g \in G$.

Proof. Fix $g \in G$. By Problem Sheet 1, the action $g_V \in \mathrm{GL}(V)$ of g on V is diagonalisable. Fix a basis of g_V-eigenvectors $\{v_1, \cdots, v_n\}$ for V with corresponding eigenvalues $\lambda_1, \cdots, \lambda_n$, and fix a basis of g_W-eigenvectors $\{w_1, \cdots, w_m\}$ for W with eigenvalues $\mu_1, \cdots, \mu_m$. Then

$$\chi_V(g) = \mathrm{tr}(g_V) = \sum_{i=1}^n \lambda_i \quad \text{and} \quad \chi_W(g) = \mathrm{tr}(g_W) = \sum_{j=1}^m \mu_j.$$

(a) Let $\{v_1^*, \cdots, v_n^*\}$ be the dual basis for V^* relative to $\{v_1, \cdots, v_n\}$. Then

$$(g \cdot v_i^*)(v_j) = v_i^*(g^{-1} \cdot v_j) = v_i^*(\lambda_j^{-1} v_j) = \lambda_j^{-1}\delta_{i,j} = (\lambda_i^{-1} v_i^*)(v_j)$$

for all $i, j = 1, \cdots, n$ shows that

$$g \cdot v_i^* = \lambda_i^{-1} v_i^* \quad \text{for all} \quad i = 1, \cdots, n.$$

But each λ_i is a *root of unity* by Problem Sheet 1, so $g \cdot v_i^* = \overline{\lambda_i} v_i^*$ and hence

$$\chi_{V^*}(g) = \mathrm{tr}(g_{V^*}) = \sum_{i=1}^n \overline{\lambda_i} = \overline{\mathrm{tr}(g_V)} = \overline{\chi_V(g)}.$$

(c) By our definition of $V \otimes W$ — see Definition 4.6 — the elementary tensors $\{v_i \otimes w_j : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ form a basis for $V \otimes W$. Using Definition 4.10,

$$g \cdot (v_i \otimes w_j) = (g \cdot v_i) \otimes (g \cdot w_j) = (\lambda_i v_i) \otimes (\mu_j w_j) = \lambda_i \mu_j (v_i \otimes w_j).$$

In other words, the elementary tensors $\{v_i \otimes w_j : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ form a basis of eigenvectors for the g-action on $V \otimes W$, with $v_i \otimes w_j$ having eigenvalue $\lambda_i \mu_j$. Therefore

$$\chi_{V \otimes W}(g) = \sum_{i=1}^n \sum_{j=1}^m \lambda_i \mu_j = \left(\sum_{i=1}^n \lambda_i\right)\left(\sum_{j=1}^m \mu_j\right) = \chi_V(g)\chi_W(g).$$

(d) By Lemma 4.11, there is a natural isomorphism of G-representations

$$V^* \otimes W \quad \xrightarrow{\cong} \quad \mathrm{Hom}(V, W).$$

Isomorphic representations have the same character. Then (a) and (c) give

$$\chi_{\mathrm{Hom}(V,W)} = \chi_{V^* \otimes W} = \chi_{V^*}\chi_W = \overline{\chi_V}\chi_W.$$

(b,e,f) We leave these to Problem Sheet 3. □

Proposition 5.22. Let V and W be finite dimensional $\mathbb{C}G$-modules. Then
(a) $\operatorname{Hom}_{\mathbb{C}G}(V,W) = \operatorname{Hom}(V,W)^G$ and
(b) $\langle \chi_V, \chi_W \rangle = \dim \operatorname{Hom}_{\mathbb{C}G}(V,W)$.

Proof. (a) Let $f \in \operatorname{Hom}(V,W)$. Then f is fixed by the G-action if and only if

$$g \cdot f(g^{-1} \cdot v) = f(v) \quad \text{for all} \quad g \in G, v \in V$$

or in other words, if and only if

$$g_W \circ f = f \circ g_V \quad \text{for all} \quad g \in G.$$

Definition 1.12 tells us that this is the same as $f \in \operatorname{Hom}_{\mathbb{C}G}(V,W)$.

(b) The key idea is to apply the Fixed Point Formula to the G-representation $\operatorname{Hom}(V,W)$ from Definition 4.4. By Proposition 5.20 and Proposition 5.21(d),

$$\dim \operatorname{Hom}(V,W)^G = \frac{1}{|G|}\sum_{g\in G} \chi_{\operatorname{Hom}(V,W)}(g) = \frac{1}{|G|}\sum_{g\in G} \overline{\chi_V(g)}\chi_W(g) = \langle \chi_V, \chi_W\rangle. \quad \square$$

We can now prove the Row Orthogonality Theorem.

Proof of Theorem 5.13. Let V and W be the simple $\mathbb{C}G$-modules whose characters are $\varphi = \chi_V$ and $\psi = \chi_W$, respectively. Since V and W are simple, Schur's Lemma (Theorem 3.4) and Lemma 2.13 together tell us that

$$\dim \operatorname{Hom}_{\mathbb{C}G}(V,W) = \begin{cases} 1 & \text{if} \quad V \cong W \\ 0 & \text{if} \quad V \ncong W. \end{cases}$$

Using Proposition 5.22, we conclude that always we have

$$\langle \varphi, \psi \rangle = \langle \chi_V, \chi_W \rangle = \dim_{\mathbb{C}G} \operatorname{Hom}(V,W) \in \{0,1\}.$$

Suppose that $\chi_V = \chi_W$. Then

$$\langle \chi_V, \chi_W \rangle = ||\chi_V||^2 = \frac{1}{|G|}\sum_{g\in G} |\chi_V(g)|^2 \geq \frac{(\dim V)^2}{|G|} > 0$$

because $\chi_V(1) = \dim V$ by Lemma 5.5(a). So in this case necessarily $\langle \chi_V, \chi_V \rangle = 1$.

Suppose now $\chi_V \neq \chi_W$. Then V cannot be isomorphic to W as isomorphic representations have the same characters, so $\langle \varphi, \psi \rangle = \dim \operatorname{Hom}_{\mathbb{C}G}(V,W) = 0$. $\square$

Next we come to another consequence of the Row Orthogonality Theorem, which will turn out to be very useful for completing character tables.

Theorem 5.23 (Column Orthogonality)**.** Let G be a finite group, let $\chi_1, \cdots, \chi_r$ be the irreducible characters of G and let $g, h \in G$. Then

$$\sum_{i=1}^{r} \overline{\chi_i(g)}\chi_i(h) = \begin{cases} |C_G(g)| & \text{if } g \text{ is conjugate to } h, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\{g_1, \cdots, g_r\}$ be a complete list of representatives for the conjugacy classes of G, recalling from Corollary 3.13 that the number $s(G)$ of these classes equals the number $r = r_{\mathbb{C}}(G)$ of isomorphism classes of simple $\mathbb{C}G$-modules.

Say $g \in g_j^G$ and $h \in g_k^G$ for some j, k. Since the characters χ_i are class functions by Lemma 5.3, we may assume that $g = g_j$ and $h = g_k$.

We have already seen in Example 5.18 that the character table viewed as a matrix $(\chi_i(g_j))$ does not quite form a unitary matrix, because we have to remember the weights $|g_j^G|/|G|$ when computing the inner product of two rows of this matrix. To fix this, we introduce a fudge factor as follows: define for each $i, j = 1, \cdots, r$

$$x_{i,j} := \chi_i(g_j) \cdot c_j \quad \text{where} \quad c_j := \sqrt{|g_j^G|/|G|}.$$

We compute that for any $i, k = 1, \cdots, r$ we have

$$\begin{array}{rcl} \sum\limits_{j=1}^r \overline{x_{i,j}}\, x_{k,j} & = & \sum\limits_{j=1}^r \overline{\chi_i(g_j)c_j}\ \chi_k(g_j)c_j \\ & = & \sum\limits_{j=1}^r \overline{\chi_i(g_j)}\chi_k(g_j)c_j^2 \\ & = & \frac{1}{|G|}\sum\limits_{j=1}^r |g_j^G|\overline{\chi_i(g_j)}\chi_k(g_j) \\ & = & \frac{1}{|G|}\sum\limits_{x\in G} \overline{\chi_i(x)}\chi_k(x) \\ & = & \langle \chi_i, \chi_k \rangle. \end{array}$$

Since $\langle \chi_i, \chi_k \rangle = \delta_{i,k}$ by the Row Orthogonality theorem, Theorem 5.13, this means that the $r \times r$ matrix $X := (x_{i,j})$ is unitary:

$$\overline{X} \cdot X^T = I.$$

So $\overline{X}$ is the left-inverse of X^T in $\mathrm{GL}_r(\mathbb{C})$. It is also the right-inverse, by Part A Linear Algebra; applying complex conjugation to $X^T \cdot \overline{X} = I$, we obtain

$$\overline{X}^T \cdot X = I.$$

Hence for any $j, k = 1, \cdots, r$, we have

$$(\overline{X}^T \cdot X)_{j,k} = \sum_{i=1}^r \overline{x_{i,j}}\, x_{i,k} = \sum_{i=1}^r \overline{\chi_i(g_j)c_j}\ \chi_i(g_k)c_k = \delta_{j,k}.$$

Divide both sides by c_jc_k: by Lemma 5.17 we have $1/c_j^2 = |G|/|g_j^G| = |C_G(g_j)|$. □

Example 5.24. Let G be the symmetric group S_4. The conjugacy class representatives are $g_1 = 1, g_2 = (12)(34), g_3 = (123), g_4 = (12), g_5 = (1234)$, with conjugacy classes of sizes $1, 3, 8, 6, 6$ respectively. We know from Problem Sheet 0 that V_4 is a normal subgroup of G with S_4/V_4 being isomorphic to the symmetric group S_3. This gives us three irreducible characters $\widetilde{\mathbb{1}}, \widetilde{\epsilon}, \widetilde{\chi_W}$ obtained by inflation from S_3

using Example 5.6(b):

g	1	g_2	g_3	g_4	g_5
$\lvert g^G\rvert$	1	3	8	6	6
$\lvert C_G(g)\rvert$	24	8	3	4	4
$\widetilde{\mathbb{1}}$	1	1	1	1	1
$\widetilde{\epsilon}$	1	1	1	-1	-1
$\widetilde{\chi_W}$	2	2	-1	0	0
χ_4	d_4	α_4	β_4	γ_4	δ_4
χ_5	d_5	α_5	β_5	γ_5	δ_5

Since $r_{\mathbb{C}}(G) = s(G) = 5$ by Corollary 3.13, we are missing two irreducible characters χ_4 and χ_5 of degrees d_4 and d_5, say. Then $d_4^2 + d_5^2 = 24 - 1^2 - 1^2 - 2^2 = 18$ by Theorem 5.23 with $g = h = 1$ (or Corollary 3.18(b)). The only solution to this equation in positive integers is $d_3 = d_4 = 3$. Now apply Theorem 5.23 to the first pair of columns and then to the second column to obtain

$$1 + 1 + 4 + 3\alpha_4 + 3\alpha_5 = 0, \quad 1^2 + 1^2 + 2^2 + |\alpha_4|^2 + |\alpha_5|^2 = 8.$$

Hence $\alpha_4 + \alpha_5 = -2$ and $|\alpha_4|^2 + |\alpha_5|^2 = 2$, and in this situation Problem Sheet 0, Question 4 tells us that $\alpha_4 = \alpha_5 = -1$. Next, Theorem 5.23 applied to the third column tells us that

$$1^2 + 1^2 + (-1)^2 + |\beta_4|^2 + |\beta_5|^2 = 3$$

whence $\beta_4 = \beta_5 = 0$. Similar considerations show that $\gamma_5 = -\gamma_4$ and that $|\gamma_4| = 1$. Now, $g_4 = (12)$ has order 2 so it acts with eigenvalues ± 1 in any representation. Hence γ_4, the sum of these eigenvalues, is a real number, so $\gamma_4 \in \{1, -1\}$. Without loss of generality, we may assume that $\gamma_4 = 1$, otherwise we can swap χ_4 with χ_5.

We conclude that the complete character table of S_4 is

g	1	g_2	g_3	g_4	g_5
$\lvert g^G\rvert$	1	3	8	6	6
$\lvert C_G(g)\rvert$	24	8	3	4	4
$\widetilde{\mathbb{1}}$	1	1	1	1	1
$\widetilde{\epsilon}$	1	1	1	-1	-1
$\widetilde{\chi_W}$	2	2	-1	0	0
χ_4	3	-1	0	1	-1
χ_5	3	-1	0	-1	1

6. Induced representations

The Row and Column orthogonality theorems, Theorems 5.13 and Theorem 5.23 are powerful tools but they are only good for completing character tables and not for constructing them. We will now introduce a powerful new technique of constructing representations of G using representations of its proper subgroups. This technique is called *induction.*

We return to the setting of kG-modules over a general field k for now.

Definition 6.1. Let H be a finite group and let V be a kH-module. The vector space of *H-coinvariants* V_H of V is

$$V_H := V/k\{h \cdot v - v : h \in H, v \in V\}.$$

Equivalently, this is the largest quotient kH-module of V which is isomorphic to a trivial module.

Whenever W is a vector space, the set $kG \otimes W$ is again a vector space which is isomorphic to a direct sum of $|G|$ copies of W. The proof of the following Lemma can be safely left as an exercise.

Lemma 6.2. Let H be a subgroup of the finite group G, let W be a kH-module.

(a) There is a linear G-action on $kG \otimes W$ given on elementary tensors by

$$g \cdot (x \otimes w) := gx \otimes w \quad \text{for all} \quad g, x \in G, w \in W.$$

We call this the *left G-action.*

(b) There is a linear H-action on $kG \otimes W$ given on elementary tensors by

$$h \star (x \otimes w) := xh^{-1} \otimes h \cdot w \quad \text{for all} \quad h \in H, x \in G, w \in W.$$

We call this the *right H-action.*

(c) The two actions commute pointwise:

$$g \cdot (h \star u) = h \star (g \cdot u) \quad \text{for all} \quad g \in G, h \in H, u \in kG \otimes W.$$

Corollary 6.3. Let H be a subgroup of the finite group G and let W be a kH-module. Then the space of H-coinvariants $(kG \otimes W)_H$ of $kG \otimes W$ with respect to the right H-action is a kG-module.

Proof. The action of G on $kG \otimes W$ preserves the subspace $(H-1) \star (kG \otimes W)$: for each $u \in kG \otimes W$, $g \in G, h \in H$ we have

$$g \cdot (h \star u - u) = h \star (g \cdot u) - (g \cdot u) \in (H-1) \star (kG \otimes W)$$

by Lemma 6.2(c). So, the G-action on $kG \otimes W$ from Lemma 6.2(a) descends to the right H-coinvariants $(kG \otimes W)_H = (kG \otimes W)/(H-1) \star (kG \otimes W)$. □

Definition 6.4. Let H be a subgroup of G and let W be a kH-module.

(a) The *induced kG-module* $\operatorname{Ind}_H^G W$ is the space of H-coinvariants

$$\operatorname{Ind}_H^G W := (kG \otimes W)_H$$

of $kG \otimes W$ under the right H-action from Lemma 6.2.

(b) We will write $g \mathbin{\overline{\otimes}} w$ to denote the image of $g \otimes w \in kG \otimes W$ in the quotient vector space $\operatorname{Ind}_H^G W = (kG \otimes W)_H$.

(c) If $\sigma : H \to \mathrm{GL}(W)$ is the representation of H afforded by W, we call the representation of G afforded by $\mathrm{Ind}_H^G W$ the *induced representation* and denote it by $\mathrm{Ind}_H^G \sigma$.

Lemma 6.5. Let $g \in G$ and $w \in W$. Then

(a) $gh \mathbin{\overline{\otimes}} w = g \mathbin{\overline{\otimes}} h \cdot w$ for all $h \in H$, and

(b) $g \cdot (x \mathbin{\overline{\otimes}} w) = gx \mathbin{\overline{\otimes}} w$ for all $x \in G$.

What does $\mathrm{Ind}_H^G W$ look like as a vector space?

Lemma 6.6. Let $x \in G$. Then $xkH \otimes W$ is an H-stable subspace of $kG \otimes W$ under the right H-action, and there is a linear isomorphism

$$\alpha : W \xrightarrow{\cong} (xkH \otimes W)_H, \quad w \mapsto x \mathbin{\overline{\otimes}} w,$$

so that $(xkH \otimes W)_H = x \mathbin{\overline{\otimes}} W$.

Proof. The first assertion is an easy exercise. By Lemma 4.9, there is a linear map $\beta : xkH \otimes W \to W$ given on elementary tensors by $\beta(xh \otimes w) = h \cdot w$ for all $h \in H$ and $w \in W$. Now for any $y \in H$ we have

$$\beta(y \star (xh \otimes w)) = \beta(xhy^{-1} \otimes y \cdot w) = (hy^{-1}) \cdot (y \cdot w) = h \cdot w.$$

Hence β is zero on $(H-1)\star(xkH \otimes W)$, so it descends to a well-defined linear map

$$\overline{\beta} : (xkH \otimes W)_H \to W, \quad xh \mathbin{\overline{\otimes}} w \mapsto h \cdot w.$$

Then using Lemma 6.5(a), we compute that for every $h \in H$ and $w \in W$,

$$\alpha(\overline{\beta}(xh \mathbin{\overline{\otimes}} w)) = \alpha(h \cdot w) = x \mathbin{\overline{\otimes}} h \cdot w = xh \mathbin{\overline{\otimes}} w.$$

Since $xkH \otimes W$ is spanned by vectors of the form $xh \otimes w$, this shows that $\alpha \circ \overline{\beta} = 1_{(xkH \otimes W)_H}$. Checking $\overline{\beta} \circ \alpha = 1_W$ is easy. Hence α is an isomorphism. □

Proposition 6.7. Let $\{x_1, \cdots, x_m\}$ be a complete set of left coset representatives for H in G so that $G = x_1H \cup \cdots \cup x_mH$.

(a) There is a vector space decomposition

$$\mathrm{Ind}_H^G W = (x_1 \mathbin{\overline{\otimes}} W) \oplus (x_2 \mathbin{\overline{\otimes}} W) \oplus \cdots \oplus (x_m \mathbin{\overline{\otimes}} W).$$

(b) We have $\dim \mathrm{Ind}_H^G W = |G : H| \dim W$.

Proof. By Lemma 6.6, $xkH \otimes W$ is an H-stable subspace of $kG \otimes W$ for the right H-action for any $x \in G$. Since G is the disjoint union of the left cosets x_iH,

$$kG \otimes W = \bigoplus_{i=1}^{m} x_i kH \otimes W.$$

The operation of taking H-coinvariants commutes with direct sums up to isomorphism. Taking H-coinvariants and applying Lemma 6.6 gives

$$\mathrm{Ind}_H^G W = (kG \otimes W)_H \cong \bigoplus_{i=1}^{m} (x_i kH \otimes W)_H = \bigoplus_{i=1}^{m} x_i \mathbin{\overline{\otimes}} W,$$

where $x_i \mathbin{\overline{\otimes}} W \cong W$ for each i. Now take dimensions. □

Example 6.8. There is a kG-linear isomorphism $k(G/H) \cong \operatorname{Ind}_H^G \mathbb{1}$ between the permutation module $k(G/H)$ from Definition 1.5 and the induced module $\operatorname{Ind}_H^G \mathbb{1}$.

Definition 6.9. Let H be a subgroup of G and let V be a kG-module. Then V is also a kH-module by restricting the action of kG to its subring kH; we denote the resulting kH-module $\operatorname{Res}_H^G V$.

In categorical terms (see Part C Category Theory), our next result tells us that "induction is left-adjoint to restriction".

Proposition 6.10. Let H be a subgroup of the finite group G, let W be a kH-module and let U be a kG-module. Then there is a linear isomorphism

$$\Phi : \operatorname{Hom}_{kG}(\operatorname{Ind}_H^G W, U) \quad \xrightarrow{\cong} \quad \operatorname{Hom}_{kH}(W, \operatorname{Res}_H^G U)$$

given by $\Phi(\alpha)(w) = \alpha(1 \mathbin{\overline{\otimes}} w)$ for all $\alpha \in \operatorname{Hom}_{kG}(\operatorname{Ind}_H^G W, U)$ and all $w \in W$.

Proof. The map $W \to \operatorname{Res}_H^G \operatorname{Ind}_H^G W$ given by $w \mapsto 1 \mathbin{\overline{\otimes}} w$ is kH-linear. Hence, given a kG-linear $\alpha : \operatorname{Ind}_H^G W \to U$, we can view α as being a kH-linear map $\operatorname{Res}_H^G \operatorname{Ind}_H^G W \to \operatorname{Res}_H^G U$ by restriction, and then precompose it with $w \mapsto 1 \mathbin{\overline{\otimes}} w$ to obtain the kH-linear map $\Phi(\alpha)$. This shows that Φ is well-defined.

We will now construct a map Ψ in the opposite direction. Take some kH-linear map $\beta : W \to \operatorname{Res}_H^G U$ and define $\Psi(\beta) : \operatorname{Ind}_H^G W \to U$ by setting

$$\Psi(\beta)(g \mathbin{\overline{\otimes}} w) := g \cdot \beta(w) \quad \text{for all} \quad w \in W, g \in G.$$

To see that this is well-defined, we must show that $gh \cdot \beta(w) = g \cdot \beta(h \cdot w)$ for all $g \in G, h \in H, w \in W$. But this follows immediately from the hypothesis that β is kH-linear. We check that $\Psi(\beta)$ is kG-linear as follows: for all $g, x \in G, w \in W$,

$$\Psi(\beta)(g \cdot (x \mathbin{\overline{\otimes}} w)) = \Psi(\beta)(gx \mathbin{\overline{\otimes}} w) = (gx) \cdot \beta(w) = g \cdot (x \cdot \beta(w)) = g \cdot \Psi(\beta)(x \mathbin{\overline{\otimes}} w).$$

Since everything in sight is linear, this defines the required linear map

$$\Psi : \operatorname{Hom}_{kH}(W, \operatorname{Res}_H^G U) \to \operatorname{Hom}_{kG}(\operatorname{Ind}_H^G W, U).$$

We now show Φ and Ψ are mutually inverse. If $\alpha : \operatorname{Ind}_H^G W \to U$ is kG-linear, then

$$\Psi(\Phi(\alpha))(g \mathbin{\overline{\otimes}} w) = g \cdot \Phi(\alpha)(w) = g \cdot \alpha(1 \mathbin{\overline{\otimes}} w) = \alpha(g \mathbin{\overline{\otimes}} w) \quad \text{for all} \quad g \in G, w \in W$$

which shows $\Psi(\Phi(\alpha)) = \alpha$, and similarly for any $\beta \in \operatorname{Hom}_{kH}(W, \operatorname{Res}_H^G U)$ we have

$$\Phi(\Psi(\beta))(w) = \Psi(\beta)(1 \mathbin{\overline{\otimes}} w) = 1 \cdot \beta(w) = \beta(w) \quad \text{for all} \quad w \in W$$

which shows that $\Phi(\Psi(\beta)) = \beta$. □

We will now again specialise to the case $k = \mathbb{C}$.

Definition 6.11. Let H be a subgroup of the finite group G.

(a) Let ψ be a character of G afforded by the $\mathbb{C}G$-module V. Then the *restricted character* is the character $\operatorname{Res}_H^G \psi$ of the $\mathbb{C}H$-module $\operatorname{Res}_H^G V$.
(b) Let φ be a character of H afforded by the $\mathbb{C}H$-module W. Then the *induced character* is the character $\operatorname{Ind}_H^G \varphi$ of the $\mathbb{C}G$-module $\operatorname{Ind}_H^G W$.

Since there are now two groups in play, we will denote the inner product on $\mathcal{C}(G)$ from Definition 5.12 by using a subscript:

$$\langle -, - \rangle_G : \mathcal{C}(G) \times \mathcal{C}(G) \to \mathbb{C}.$$

Corollary 6.12 (Frobenius Reciprocity)**.** Let φ be a character of H and let ψ be a character of G. Then

$$\langle \operatorname{Ind}_H^G \varphi, \psi \rangle_G = \langle \varphi, \operatorname{Res}_H^G \psi \rangle_H.$$

Proof. Let U be the $\mathbb{C}G$-module whose character is ψ, and let W be the $\mathbb{C}H$-module whose character is φ. Applying Proposition 5.22 twice, we have

$$\begin{array}{rcl} \langle \operatorname{Ind}_H^G \varphi, \psi \rangle_G & = & \dim \operatorname{Hom}_{\mathbb{C}G}(\operatorname{Ind}_H^G W, U), \quad \text{and} \\ \langle \varphi, \operatorname{Res}_H^G \psi \rangle_H & = & \dim \operatorname{Hom}_{\mathbb{C}H}(W, \operatorname{Res}_H^G U). \end{array}$$

Now apply Proposition 6.10. □

Example 6.13. Let U be a simple $\mathbb{C}G$-module and consider the trivial character $\mathbb{1}$ of $H := \{1\}$. Then $\operatorname{Ind}_H^G \mathbb{1}$ is the character of the free $\mathbb{C}G$-module of rank 1 by Example 6.8. Then Frobenius Reciprocity tells us that

$$\langle \operatorname{Ind}_H^G \mathbb{1}, \chi_U \rangle_G = \langle \mathbb{1}, \operatorname{Res}_H^G \chi_U \rangle_H = \dim U.$$

In other words, U appears in $\mathbb{C}G$ precisely $\dim U$ times. We knew this already — see Corollary 3.18(a).

Since $\psi(h)$ is the trace of the action of an element $h \in H$ on U, it is clear that $\operatorname{Res}_H^G \psi$ is simply the restriction of the class function $\psi \in \mathcal{C}(G)$ to H; the resulting function on H is still constant on H-conjugacy classes and in this way we have a natural linear map

$$\operatorname{Res}_H^G : \mathcal{C}(G) \to \mathcal{C}(H).$$

Corollary 6.12 suggests that there is linear map in the opposite direction

$$\operatorname{Ind}_H^G : \mathcal{C}(H) \to \mathcal{C}(G)$$

which is an adjoint for Res_H^G in the sense of Part A Linear Algebra. To see that this is indeed the case, we must compute the character of our induced module $\operatorname{Ind}_H^G W$. We start this calculation with the following Lemma.

Lemma 6.14. Let H be a subgroup of the finite group G. Let $\{x_1, \cdots, x_m\}$ be a complete set of left coset representatives for H in G so that $G = x_1 H \cup \cdots \cup x_m H$. For each $g \in G$, write

$$g x_i H = x_{g \cdot i} H \quad \text{for all} \quad i = 1, \ldots, m$$

for some permutation $i \mapsto g \cdot i$ of $\{1, \cdots, m\}$. Define

$$\mathrm{Fix}(g) := \{i \in \{1, \cdots, m\} : g \cdot i = i\}$$

to be the fixed-point set of g in its action on $\{1, \cdots, m\}$. Then for every finite dimensional $\mathbb{C}H$-module W, we have

(a) $g \cdot (x_i \overline{\otimes} W) \subseteq x_{g \cdot i} \overline{\otimes} W$ for all $i = 1, \cdots, m$, and
(b) $(\mathrm{Ind}_H^G \chi_W)(g) = \sum\limits_{i \in \mathrm{Fix}(g)} \chi_W(x_i^{-1} g x_i)$.

Proof. (a) Using Lemma 6.5, we have

$$g \cdot (x_i \overline{\otimes} w) = g x_i \overline{\otimes} w = x_{g \cdot i}(x_{g \cdot i}^{-1} g x_i) \overline{\otimes} w = x_{g \cdot i} \overline{\otimes} (x_{g \cdot i}^{-1} g x_i) \cdot w \in x_{g \cdot i} \overline{\otimes} W$$

for any $i = 1, \cdots, m$ and any $w \in W$.

(b) Let $\rho : G \to \mathrm{GL}(\mathrm{Ind}_H^G W)$ be the representation afforded by the $\mathbb{C}G$-module $\mathrm{Ind}_H^G W$. Then by Proposition 6.7(a) we have a decomposition of vector spaces

$$\mathrm{Ind}_H^G W = (x_1 \overline{\otimes} W) \oplus (x_2 \overline{\otimes} W) \oplus \cdots \oplus (x_m \overline{\otimes} W)$$

and by part (a), $\rho(g)$ permutes the direct summands $x_i \overline{\otimes} W$ in the same way as g permutes the numbers $\{1, \cdots, m\}$ (or equivalently, in the same way as g permutes the left cosets G/H). Writing down the matrix of $\rho(g)$ with respect to a choice of basis for $\mathrm{Ind}_H^G W$ which respects the direct sum decomposition, we see that the block matrices on the diagonal corresponding to the indices i that are *not* fixed by g are all zero. However if $g \cdot i = i$ then $\rho(g)$ preserves $x_i \overline{\otimes} W$, and its restriction to this subspace has trace equal to the trace of the action of $x_i^{-1} g x_i \in H$ on W. □

It turns out that there is a more invariant way of expressing the result of this calculation, which does not depend on the choice of coset representatives.

Definition 6.15. For each $\varphi : H \to \mathbb{C}$, define its *extension by zero to G* to be the function $\varphi^\circ : G \to \mathbb{C}$ which agrees with φ on H and which is zero on $G \backslash H$.

Theorem 6.16. Let H be a subgroup of the finite group G and let W be a finite dimensional $\mathbb{C}H$-module. Then for all $g \in G$ we have

$$(\mathrm{Ind}_H^G \chi_W)(g) = \frac{1}{|H|} \sum_{x \in G} \chi_W^\circ(x^{-1} g x).$$

Proof. Fix $g \in G$. Using the notation of Lemma 6.14, we note that $i \in \mathrm{Fix}(g) \Leftrightarrow g x_i H = x_i H \Leftrightarrow x_i^{-1} g x_i \in H$. So, we can rewrite Lemma 6.14(b) as follows:

$$(\mathrm{Ind}_H^G \chi_W)(g) = \sum_{i \in \mathrm{Fix}(g)} \chi_W(x_i^{-1} g x_i) = \sum_{i=1}^{m} \chi_W^\circ(x_i^{-1} g x_i).$$

Note that $\chi_W^\circ(h^{-1} y h) = \chi_W^\circ(y)$ for any $h \in H$ and any $y \in G$ because χ_W is a class function on H and because both H and $G \backslash H$ are stable under conjugation by

H. Therefore $\chi_W^\circ((x_ih)^{-1}g(x_ih)) = \chi_W^\circ(x_i^{-1}gx_i)$ for any $h \in H$, so

$$\sum_{x\in G} \chi_W^\circ(x^{-1}gx) = \sum_{i=1}^m \sum_{h\in H} \chi_W^\circ((x_ih)^{-1}g(x_ih)) = |H| \sum_{i=1}^m \chi_W^\circ(x_i^{-1}gx_i). \qquad \square$$

Remark 6.17. It could very well happen that $g^G \cap H = \emptyset$. In this case, Theorem 6.16 tells us that $(\operatorname{Ind}_H^G \chi_W)(g) = 0$.

Corollary 6.18. *Let H be a subgroup of G. For each $\varphi \in \mathcal{C}(H)$, define*

$$(\operatorname{Ind}_H^G \varphi)(g) := \frac{1}{|H|} \sum_{x\in G} \varphi^\circ(x^{-1}gx).$$

Then $\operatorname{Ind}_H^G : \mathcal{C}(H) \to \mathcal{C}(G)$ is left adjoint to the map $\operatorname{Res}_H^G : \mathcal{C}(G) \to \mathcal{C}(H)$ which sends $\psi \in \mathcal{C}(G)$ to its restriction $\psi_{|H} : H \to \mathbb{C}$:

$$\langle \operatorname{Ind}_H^G \varphi, \psi\rangle_G = \langle \varphi, \operatorname{Res}_H^G \psi\rangle_H \quad \text{for all} \quad \varphi \in \mathcal{C}(G), \psi \in \mathcal{C}(H).$$

Proof. The formula holds true when φ and ψ are characters of representations of H and G, respectively, by Frobenius Reciprocity (Corollary 6.12) together with Theorem 6.16. The result follows because characters of representations span class functions, by Corollary 5.15. □

As an exercise, prove Corollary 6.18 directly. For practical calculations, the following reformulation of Theorem 6.16 will be useful.

Corollary 6.19. *Let H be a subgroup of G. Let $g \in G$, and let $\{h_1, \cdots, h_\ell\}$ be a complete set of representatives for the conjugacy classes in H contained in $g^G \cap H$:*

$$g^G \cap H = h_1^H \cup \cdots \cup h_\ell^H.$$

Then for every finite dimensional $\mathbb{C}H$-module W,

$$\chi_{\operatorname{Ind}_H^G W}(g) = \frac{|G|}{|H|} \sum_{i=1}^\ell \frac{|h_i^H|}{|g^G|} \chi_W(h_i).$$

Proof. Consider the set $S := \{x \in G : x^{-1}gx \in H\}$. We can rewrite it as follows:

$$S = \bigcup_{y\in g^G\cap H} \{x \in G : x^{-1}gx = y\}.$$

For a fixed $y = x_0^{-1}gx_0 \in g^G \cap H$, there is a bijection $C_G(g) \to \{x \in G : x^{-1}gx = y\}$ given by $z \mapsto zx_0$. Applying Theorem 6.16, we obtain

$$\begin{aligned} |H|\chi_{\operatorname{Ind}_H^G W}(g) &= \sum_{x\in S} \chi_W(x^{-1}gx) = \sum_{i=1}^{\ell} \sum_{y\in h_i^H} |C_G(g)|\chi_W(y) \\ &= |C_G(g)| \sum_{i=1}^{\ell} |h_i^H| \chi_W(h_i). \end{aligned}$$

Now divide by $|H|$ and apply Lemma 5.17. □

Next, we specialise to the case where we have a *normal* subgroup N of G. In this case, conjugation by any $x \in G$ preserves N.

Definition 6.20. Let N be a normal subgroup of G, let $s \in G$ and let $\varphi : N \to \mathbb{C}$. The *$x$-twist* of φ is the function

$$\varphi^x : N \to \mathbb{C}, \quad h \mapsto \varphi(x^{-1}hx).$$

Since conjugation by $x \in G$ is an automorphism of N, it permutes the conjugacy classes of N, so $\varphi^x \in \mathcal{C}(N)$ whenever $\varphi \in \mathcal{C}(N)$. When $\varphi \in \mathcal{C}(N)$, φ^x only depends on $xN \in G/N$. This defines a permutation action of G/N on $\mathcal{C}(N)$, via

$$xN \cdot \varphi = \varphi^x \quad \text{for all} \quad xN \in G/N, \varphi \in \mathcal{C}(N).$$

Proposition 6.21. Let φ be a character of the normal subgroup N of G. Then

(a) φ^x is another character of N, and

(b) $\operatorname{Res}_N^G \operatorname{Ind}_N^G \varphi = \varphi^{x_1} + \cdots + \varphi^{x_m}$, where $\{x_1, \cdots, x_m\}$ is a complete set of left coset representatives for N in G.

Proof. Let W be the $\mathbb{C}N$-module with character φ, let $h \in N$ and fix $i = 1, \cdots, m$. Since N is normal, $hx_iN = x_i(x_i^{-1}hx_iN) = x_iN$ shows that multiplication by h fixes each point of G/N. So, Lemma 6.14 implies that $x_i \mathbin{\overline{\otimes}} W$ is stable under the action of N, so $x_i \mathbin{\overline{\otimes}} W$ is another $\mathbb{C}N$-module. In fact, the decomposition of $\operatorname{Res}_N^G \operatorname{Ind}_N^G W$ into a direct sum of vector subspaces $x_i \mathbin{\overline{\otimes}} W$ from Lemma 6.7 is a decomposition into a direct sum of $\mathbb{C}N$-modules, so

$$\operatorname{Res}_N^G \operatorname{Ind}_N^G \chi_W = \sum_{i=1}^{m} \chi_{x_i \mathbin{\overline{\otimes}} W}.$$

But $\chi_{x_i \mathbin{\overline{\otimes}} W} = \chi_W^{x_i}$ by the proof of Lemma 6.14(b). □

We can now give a construction of irreducible characters using induction.

Corollary 6.22. Let φ be an irreducible character of the normal subgroup N of G, such that $\varphi^x \neq \varphi$ for all $x \in G \backslash N$. Then the character $\operatorname{Ind}_N^G \varphi$ is irreducible.

Proof. We use Frobenius Reciprocity, Corollary 6.12, to compute $|| \operatorname{Ind}_N^G \varphi||^2$:

$$\langle \operatorname{Ind}_N^G \varphi, \operatorname{Ind}_N^G \varphi \rangle_G = \langle \operatorname{Res}_N^G \operatorname{Ind}_N^G \varphi, \varphi \rangle_N.$$

But $\operatorname{Res}_N^G \operatorname{Ind}_N^G \varphi = \varphi^{x_1} + \cdots + \varphi^{x_m}$ by Proposition 6.21, where $G = \bigcup_{i=1}^{m} x_iN$. We may assume that $x_1 = 1$; our assumption $\varphi^x \neq \varphi$ for all $x \in G \backslash N$ then implies that $\varphi^{x_i} \neq \varphi$ for $i \geq 2$. Because each φ^{x_i} is irreducible, $\langle \varphi, \varphi \rangle_N = 1$ and $\langle \varphi^{x_i}, \varphi \rangle_N = 0$ for $i \geq 2$ by Theorem 5.13. Hence $|| \operatorname{Ind}_N^G \varphi||^2 = 1$ and now we can use Corollary 5.15 to deduce that $\operatorname{Ind}_N^G \varphi$ is irreducible. □

Using Corollary 6.22, we can now find all irreducible characters of the dihedral groups D_{2n}. We only treat the case where $n = 2m + 1$ is odd, and leave the even case as an exercise.

Example 6.23. Let G be the dihedral group of order $4m + 2$ for some $m \geq 1$. Then G has m irreducible characters of degree 2, and two linear characters.

Proof. Write $G = \langle r, s : r^{2m+1} = s^2 = 1, srs^{-1} = r^{-1}\rangle$ and note that $N := \langle r\rangle$ is a normal cyclic subgroup of G of order $2m+1$. By Lemma 5.10, N has $2m+1$ linear characters $\{\varphi^i : 0 \leqslant i \leqslant 2m\}$ where $\varphi : N \to \mathbb{C}^\times$ sends r to some fixed primitive $(2m+1)$th root of unity ζ, say. We calculate

$$(\varphi^i)^s(r^j) = \varphi^i(s^{-1}r^js) = \varphi^i(r^{-j}) = \zeta^{-ij} = \varphi^{2m+1-i}(r^j) \quad \text{for all} \quad i, j = 0, \cdots, 2m.$$

So, the trivial character $\mathbb{1} = \varphi^0$ of N is fixed under the conjugation action of G on $\mathcal{C}(N)$, and the other irreducible characters $\{\varphi_1, \cdots, \varphi_{2m}\}$ break up into m orbits of size 2. For each $i = 1, \cdots, m$, the induced character

$$\chi_i := \operatorname{Ind}_N^G \varphi^i$$

is irreducible by Corollary 6.22, and its restriction back to N is equal to $\varphi^i + \varphi^{2m+1-i}$ by Proposition 6.21(b). This implies that $\chi_1, \cdots, \chi_m$ are pairwise distinct degree 2 characters of G, by Proposition 6.7(b). Inflation from the cyclic group G/N of order 2 gives two distinct linear characters of G — see Definition 5.8. Since

$$\sum_{i=1}^{m} \chi_i(1)^2 + 1^2 + 1^2 = 4m + 2 = |G|,$$

Corollary 3.18(b) says that we have found all of the irreducible characters of G. □

7. Algebraic integers and Burnside's $p^\alpha q^\beta$ theorem

Definition 7.1. Let $z \in \mathbb{C}$.

(a) We say that z is an *algebraic number* if z satisfies a polynomial equation with rational coeffcients.

(b) We say that z is an *algebraic integer* if z satisfies a *monic* polynomial equation with *integer* coefficients.

(c) The set of algebraic integers is denoted $\mathbb{A}$.

From Part A Rings and Modules, we know that the set of algebraic numbers is the union of all subfields of $\mathbb{C}$ of finite dimension as a $\mathbb{Q}$-vector space.

Examples 7.2.

(a) Every integer $a \in \mathbb{Z}$ is an algebraic integer, being a root of $t - a = 0$.

(b) Every root of unity is an algebraic integer.

(c) If z is an algebraic number, then mz is an algebraic integer for some integer m.

(d) A rational number $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$. To see this, write $\alpha = r/s$ with r, s coprime integers and suppose that

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

for some $a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z}$. Clearing denominators we obtain the equation

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1} + a_0s^n = 0$$

and therefore s divides r^n. Since s and r are coprime, this is only possible if $s = \pm 1$ and then α is an integer.

We have the following remarkable and fundamental fact.

Theorem 7.3. Algebraic integers form a subring of $\mathbb{C}$.

The heart of the proof of Theorem 7.3 is the following useful

Proposition 7.4. Let M be a finitely generated subgroup of $(\mathbb{C}, +)$. Then

$$\{z \in \mathbb{C} : zM \subseteq M\} \quad \subset \quad \mathbb{A}.$$

Proof. Suppose $zM \subseteq M$. Choose a generating set $\{v_1, \cdots, v_d\}$ for M and write

$$zv_i = \sum_{j=1}^{d} u_{ij} v_j \quad \text{for all} \quad i = 1, \cdots, d \tag{7.1}$$

for some integers $u_{ij} \in \mathbb{Z}$. Consider the characteristic polynomial $g(t) := \det(tI - U)$ of the $d \times d$ matrix $U = (u_{ij})$. Since all entries of U are integers, $g(t)$ is a *monic* polynomial with *integer* coefficients. We can rewrite (7.1) as a matrix equation

$$U\mathbf{v} = z\mathbf{v}$$

where $\mathbf{v} = (v_1, \cdots, v_d)^T$. Hence z is an eigenvalue of U, so $g(z) = \det(zI - U) = 0$ and z is an algebraic integer. □

Proof of Theorem 7.3. Let $\alpha, \beta \in \mathbb{A}$; we have to show that $\alpha\beta \in \mathbb{A}$ and $\alpha + \beta \in \mathbb{A}$. Choose integers $a_0, \cdots, a_{m-1}$ and $b_0, \cdots, b_{n-1}$ such that

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0 \quad \text{and} \quad \beta^n + b_{m-1}\beta^{m-1} + \cdots + b_1\beta + b_0 = 0$$

and consider the abelian subgroup M of $\mathbb{C}$ generated by the set $\{\alpha^i\beta^j : 0 \leqslant i < m, 0 \leqslant j < n\}$. The monic polynomial equations satisfied by α and β ensure that

$$\alpha M \subseteq M \quad \text{and} \quad \beta M \subseteq M.$$

Since M is an additive subgroup of $\mathbb{C}$, we deduce that

$$(\alpha\beta)M \subseteq M \quad \text{and} \quad (\alpha + \beta)M \subseteq M.$$

Hence $\alpha\beta$ and $\alpha + \beta \in \mathbb{A}$ by Proposition 7.4. □

Next we return to representation theory and extract some algebraic integers from the complex group ring of a finite group.

Lemma 7.5. Let χ be a character of the finite group G. Then $\chi(g)$ is an algebraic integer for all $g \in G$.

Proof. We know that $\chi(g)$ is a sum of n-th roots of unity where n is the order of g. Since these are all algebraic integers, we can now apply Theorem 7.3. □

Recall the *conjugacy class sums* from Proposition 3.12.

Lemma 7.6. Let G be a finite group and let $C_1, \cdots, C_r$ be the conjugacy classes in G. Let S be the additive subgroup of $\mathbb{C}G$ generated by the conjugacy class sums $\widehat{C_1}, \cdots, \widehat{C_r}$. Then S is a subring of $Z(\mathbb{C}G)$.

Proof. We know that each $\widehat{C_i}$ is central in $\mathbb{C}G$ by Proposition 3.12, so it will be enough to show that S is stable under multiplication. Fix $i, j = 1, \cdots, r$. Write

$$\widehat{C_i}\widehat{C_j} = \left(\sum_{x \in C_i} x\right)\left(\sum_{y \in C_j} y\right) = \sum_{k=1}^{r} \sum_{z \in C_k} a_{ijk}(z) z$$

for some $a_{ijk}(z) \in \mathbb{C}$. Now actually $a_{ijk}(z) = |\{(x, y) \in C_i \times C_j : xy = z\}| \in \mathbb{N}$, which implies that $a_{ijk}(z) = a_{ijk}(z^g)$ for any $z \in C_k$ and any $g \in G$. So $a_{ijk} := a_{ijk}(z)$ does not depend on z. Hence

$$\widehat{C_i}\widehat{C_j} = \sum_{k=1}^{r} a_{ijk}\widehat{C_k} \in S \quad \text{for all} \quad i, j = 1, \cdots, r.$$

Since S is generated by the $\widehat{C_i}$s as an abelian group, we conclude that $S \cdot S \subseteq S$. $\square$

We will now compute the value of the central characters of simple $\mathbb{C}G$-modules — see Definition 3.5 — on our conjugacy class sums. These values turn out to be algebraic integers!

Theorem 7.7. Let V be a simple $\mathbb{C}G$-module and let $g \in G$.

(a) The conjugacy class sum $\widehat{g^G}$ acts on V by the scalar $\frac{|g^G|\chi_V(g)}{\chi_V(1)} \in \mathbb{C}$:

$$\widehat{g^G} \cdot v = \frac{|g^G|\chi_V(g)}{\chi_V(1)} \cdot v \quad \text{for all} \quad v \in V.$$

(b) This scalar is an algebraic integer.

Proof. (a) Since V is a simple $\mathbb{C}G$-module and since the conjugacy class sum $z := \widehat{g^G}$ is central in $\mathbb{C}G$, it acts by a scalar $z_V \in \mathbb{C}$ on every simple $\mathbb{C}G$-module by Schur's Lemma, Theorem 3.4. Now take the trace of this action to obtain

$$z_V \dim V = |g^G|\chi_V(g).$$

Part (a) now follows because $\dim V = \chi(1)$ by Lemma 5.5(a).

(b) Let $\rho : G \to \mathrm{GL}(V)$ be the representation afforded by V. Then ρ extends to a $\mathbb{C}$-algebra homomorphism $\widetilde{\rho} : \mathbb{C}G \to \mathrm{End}(V)$ by Question 3(a) on Problem Sheet 3. The restriction of this homomorphism to the centre $Z(\mathbb{C}G)$ is the central character of V, so $\widetilde{\rho}(Z(\mathbb{C}G)) \subseteq \mathbb{C}$. So $\widetilde{\rho}(S)$ is a finitely generated abelian subgroup of $\mathbb{C}$. But it is also a subring of $\mathbb{C}$ because $\widetilde{\rho}$ is a ring homomorphism and because S is a subring of $Z(\mathbb{C}G)$ by Lemma 7.6. Hence $z_V \cdot \widetilde{\rho}(S) \subseteq \widetilde{\rho}(S)$. Proposition 7.4 now tells us that z_V is an algebraic integer. $\square$

This theorem has the following interesting consequence.

Corollary 7.8. If V is a simple $\mathbb{C}G$-module, then $\dim V$ divides $|G|$.

Proof. By Theorem 5.13, we have $\langle \chi_V, \chi_V \rangle = 1$. Letting $g_1, \cdots, g_r$ be a complete set of representatives for the conjugacy classes of G. Using Proposition 5.21(a), we can rewrite this orthogonality relation as follows:

$$\sum_{i=1}^{r} \chi_V(g_i^{-1}) \cdot \frac{|g_i^G| \chi_V(g_i)}{\chi_V(1)} = \frac{|G|}{\chi_V(1)}.$$

Now $\chi_V(g_i^{-1})$ is an algebraic integer by Lemma 7.5, and the other factor is an algebraic integer by Theorem 7.7(b). Therefore $|G|/\chi_V(1)$ is an algebraic integer by Theorem 7.3. Since it is also a rational number, it must be an integer by Example 7.2(d). □

We will now apply our knowledge of the value of the central characters of irreducible complex G-representations on conjugacy class sums to obtain an interesting group-theoretic application of representation theory.

Theorem 7.9 (Burnside, 1904)**.** Let G be a non-abelian group of order $p^\alpha q^\beta$ where p, q are primes. Then G is not a simple group.

We begin the proof by recalling Sylow theory from Part A Group Theory.

Definition 7.10. Let G be a finite group and let p be a prime. Write $|G| = p^\alpha m$ where $p \nmid m$. A *Sylow p-subgroup* of G is a subgroup P of G of order p^α.

Sylow's three theorems are as follows.

Theorem 7.11 (Sylow, 1874)**.** Let G be a finite group.

(a) G contains at least one Sylow p-subgroup.
(b) Any two Sylow p-subgroups are conjugate in G.
(c) The number of Sylow p-subgroups of G is congruent to 1 mod p, and this number divides $m = |G|/p^\alpha$.

The first step in the proof of Burnside's Theorem is the following Lemma.

Lemma 7.12. Let G be a group of order $p^\alpha q^\beta$ where p, q are distinct primes and $\alpha, \beta \geq 1$. Let g be a central element of a Sylow p-subgroup P of G. Then $|g^G|$ is a power of q.

Proof. Since P centralises g, we have $P \leqslant C_G(g)$. So $[G : C_G(g)]$ divides $|G|/|P| = q^\beta$. But this index equals $|g^G|$ by Lemma 5.17. □

We will actually prove the following general result about finite simple groups.

Theorem 7.13. Let G be a finite group and suppose that the size of a conjugacy class of a non-central element $g \in G$ is a power of q. Then G is not a simple group.

The proof of this statement requires a little Galois Theory.

Lemma 7.14. Let $\zeta_1, \cdots, \zeta_n$ be roots of unity and let $\alpha := \frac{\zeta_1 + \cdots + \zeta_n}{n}$. Suppose also that α is an algebraic integer. Then either $\alpha = 0$, or $\alpha = \zeta_1 = \cdots = \zeta_n$.

Proof (Non-examinable). We may assume that $\zeta_1, \cdots, \zeta_n \in \mathbb{Q}(\omega)$ for some primitive k-th root of unity ω. Let $\mathcal{G}$ be the Galois group of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, and consider the *norm of* α, which is defined as follows:

$$a := \mathrm{Norm}_{\mathbb{Q}(\omega)/\mathbb{Q}}(\alpha) := \prod_{\sigma \in \mathcal{G}} \sigma(\alpha).$$

On the one hand, because each $\sigma(\zeta_j)$ is a root of unity, we have $|\sigma(\zeta_j)| = 1$ for all $j = 1, \cdots, n$ and all $\sigma \in \mathcal{G}$. Hence $|\sigma(\alpha)| \leqslant 1$ for each $\sigma \in \mathcal{G}$, so

$$|a| = \prod_{\sigma \in \mathcal{G}} |\sigma(\alpha)| \leqslant 1.$$

On the other hand, clearly a is fixed by the action of $\mathcal{G}$, and Galois Theory tells us that this means that $a \in \mathbb{Q}(\omega)^{\mathcal{G}} = \mathbb{Q}$. By our hypothesis, α is an algebraic integer, so $\sigma(\alpha)$ is also an algebraic integer for any $\sigma \in \mathcal{G}$. So, a is again an algebraic integer by Theorem 7.3. Hence $a \in \mathbb{Z}$ by Example 7.2(d).

These two facts force $a \in \{-1, 0, 1\}$. If $\alpha \neq 0$ then $|a| = 1$, so $|\zeta_1 + \cdots + \zeta_n| = n$. By the solution to Question 5(a) on Problem Sheet 3, $\alpha = \zeta_1 = \cdots = \zeta_n$. □

Proof of Theorem 7.13. The idea will be to examine all of the non-trivial irreducible representations $\rho_2, \cdots, \rho_r$ of G and show that for at least one of these, $\rho_i : G \to \mathrm{GL}(V_i)$ say, the linear map $\rho_i(g)$ is a scalar multiple of the identity: $g \in \rho_i^{-1}(\mathbb{C}^\times)$. Once we have done this, we can consider the following two *normal* subgroups of G:

$$\ker \rho_i \leqslant \rho_i^{-1}(\mathbb{C}^\times).$$

We know that $\ker \rho_i$ is a proper subgroup of G since ρ_i is non-trivial. We also know that $\rho_i^{-1}(\mathbb{C}^\times)$ is non-trivial. So, the only way G could still be a simple group is if $\ker \rho_i$ is trivial and $\rho_i^{-1}(\mathbb{C}^\times) = G$. But then $\rho_i(G) \leqslant \mathbb{C}^\times$, and G would be isomorphic to a subgroup of $\mathbb{C}^\times$ which is abelian — this contradicts our hypothesis that $g \in G$ is non-central.

Let χ_i be the character of ρ_i and consider the Column Orthogonality relation for the pair 1 and g given by Theorem 5.23:

$$1 + \sum_{i=2}^{r} \chi_i(1)\chi_i(g) = 0.$$

If all of degrees $\chi_i(1)$ were divisible by q, then we would deduce from Lemma 7.5 and Theorem 7.3 that $-1/q \in \mathbb{A}$, which contradicts Example 7.2(d). The same reasoning shows that $\chi_i(g) \neq 0$ *and* $q \nmid \chi_i(1)$ for at least one index i.

Since $|g^G|$ is a power of q, $\chi_i(1)$ is coprime to $|g^G|$. By Bezout's Lemma we can find integers a, b such that $a|g^G| + b\chi_i(1) = 1$. Hence

$$a\frac{|g^G|\chi_i(g)}{\chi_i(1)} + b\,\chi_i(g) = \frac{\chi_i(g)}{\chi_i(1)}$$

Now $|g^G|\chi_i(g)/\chi_i(1) \in \mathbb{A}$ by Theorem 7.7(b) and $\chi_i(g) \in \mathbb{A}$ by Lemma 7.5, and then Theorem 7.3 then forces $\chi_i(g)/\chi_i(1)$ to also be an algebraic integer. Since it is nonzero, Lemma 7.14 tells us that the eigenvalues of $\rho_i(g)$ are all equal to some root of unity ζ. Then $\rho_i(g) = \zeta 1_{V_i}$ is a scalar multiple of the identity as claimed. □

The proof of Burnside's Theorem is now a formality.

Proof of Theorem 7.9. We may assume $\alpha, \beta \geq 1$. By Sylow's Theorem, Theorem 7.11(a), G has a Sylow p-subgroup P. Since P is a non-trivial p-group (as $\alpha \geq 1$), it must have a non-trivial central element $g \in Z(P)$. If this element is also central in G then $\langle g \rangle$ will be a non-trivial proper normal subgroup of G (as $\beta \geq 1$) and we're done. Otherwise, g is not central in G and Lemma 7.12 tells us that $|g^G|$ is a power of q. Now apply Theorem 7.13. □