Introduction to representation theory of finite groups

Alex Bartel

28th October 2021

Contents

1 Group representations – the first encounter

These notes are about classical (ordinary) representation theory of finite groups. They accompanied a lecture course with the same name, which I held at POSTECH during the first semester 2011, although they lack many of the examples discussed in lectures. The theory presented here lays a foundation for a deeper study of representation theory, e.g. modular and integral representation theory, representation theory of more general groups, like Lie groups, or, even more generally, of algebras, and also more advanced topics.

1.1 Historical introduction

We begin with a little historical introduction. Up until the 19th century, mathematicians did not have the concept of an abstract group, but they had worked with groups in various guises. Some abelian groups had featured in Gauss's work, but more prominently, people had worked with and wondered about symmetry groups of geometric objects for a long time, e.g. the symmetry group of a regular n-gon or of the cube. In the first half of the 19th century, the then 19 year old *Évariste Galois* had the groundbreaking insight, that solutions of polynomials could be thought of as "vertices" that exhibited certain symmetries. He thereby hugely expanded the meaning of the word "symmetry" and along the way to founding what is now known as Galois theory, he introduced the abstract notion of a group. Later, in 1872, the German mathematician *Felix Klein* connected groups and geometry in a totally new way in announcing his so-called *Erlanger Programm*, where he proposed a way of using abstract group theory to unify the various geometries that had emerged in the course of the century.

By the end of the 19th century, the stage was set for standing the relationship between groups and symmetries on its head: a group had originally been just a set of symmetries of some geometric object, together with a rule of how to compose symmetries. It then acquired a life of its own as an abstract algebraic gadget. Of course, it could still act through symmetries on the same geometric object. But the same group can act on many different objects and it is a natural question whether one can describe all sensible actions of a given group. When we restrict attention to linear actions on vector spaces, we arrive at the subject of representation theory.

In these notes, we will be mainly concerned with actions of finite groups on complex vector spaces. The main achievement of this subject is the so-called character theory. The development of character theory actually started from a rather unexpected direction. In 1896, the German algebraist and number theorist *Richard Dedekind* posed the following problem to *Ferdinand Georg Frobenius*, an eminent German group theorist.

Let $G = \{g_1, \ldots, g_n\}$ be a finite group. Consider n indeterminates $x_{g_1}, \ldots, x_{g_n}$ indexed by the elements of this group. The determinant of the $n \times n$ matrix $(x_{g_i g_j^{-1}})$ is a homogeneous degree n polynomial in these indeterminates. How does it factor into irreducible components? Dedekind himself had answered this question very elegantly in the case when G is an abelian group. The polynomial then decomposes into linear factors of the form $\chi(g_1)x_{g_1} + \ldots + \chi(g_n)x_{g_n}$, one such factor for each homomorphism $\chi : G \to \mathbb{C}^\times$ (it is easy to see that there are exactly n such homomorphisms – see first exercise sheet). He told Frobe-

nius in successive letters, that he had also looked at non-abelian groups and that there, irreducible factors of degree higher than 1 appeared. Frobenius was intrigued by the question and immediately set out to work on it. Within one year, he produced three papers on the subject, in which he invented character theory of finite groups and completely answered Dedekind's question! It is worth remembering that at that time, Frobenius wasn't so much interested in group representations. It just so happens that the question posed by Dedekind is one of the many surprising applications of representation theory to the study of groups.

1.2 First definitions and examples

Throughout these notes, G denotes a group and K denotes a field.

Definition 1.1. An n-dimensional *representation* of G over K ($n \geq 1$) is a group homomorphism $\phi : G \to \mathrm{GL}(V)$, where V is an n-dimensional vector space over K and $\mathrm{GL}(V)$ denotes the group of invertible linear maps $V \to V$.

In other words, a representation is a rule, how to assign a linear transformation of V to each group element in a way that is compatible with the group operation. Via this rule, G acts on the vector space V. For $g \in G$ and $v \in V$, one often writes $g \cdot v$, or gv, or $g(v)$, or v^g instead of $\phi(g)(v)$. We also often refer to V itself as the representation, but remember that the important information is how G acts on V.

Example 1.2.

1. For any group G and any field K, the map
$$\phi : G \longrightarrow \mathrm{GL}_1(K) = K^\times, \;\; g \mapsto 1 \; \forall g \in G$$
is a representation. This is called the *trivial representation* of G (over K).

2. Let $G = C_2 = \{1, g\}$ be the cyclic group of order 2. For any field K,
$$\phi : G \longrightarrow \mathrm{GL}_1(K) = K^\times, \;\; g \mapsto -1$$
is a representation.

3. The dihedral group $D_{2n} = \langle \sigma, \tau | \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ naturally acts on the regular n-gon and this induces an action on $\mathbb{R}^2$ or $\mathbb{C}^2$ via
$$\sigma \mapsto \begin{pmatrix} \cos 2\pi/n & \sin 2\pi/n \\ -\sin 2\pi/n & \cos 2\pi/n \end{pmatrix}, \tau \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
which defines a two-dimensional representation of D_{2n}.

4. Let $Q_8 = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$ be the quaternion group. You can verify that
$$x \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
is a representation of Q_8 (you have to check that the two matrices satisfy the same relations as x and y).

5. Let G be a finite group and let $X = \{x_1, \ldots, x_n\}$ be a finite set on which G acts. Over any field K, consider an n-dimensional vector space V with a basis indexed by elements of X: $v_{x_1}, \ldots, v_{x_n}$. We can let G act on V by $g(v_x) = v_{g(x)}$ for all $x \in X$ and $g \in G$. Thus, G permutes the basis elements. This is called the *permutation representation* over K attached to X and is denoted by $K[X]$. A special (although not very special, as it turns out) case of this is if X is the set of cosets G/H for some subgroup H of G, with the usual left regular action $g(kH) = (gk)H$. Then we get the permutation representation attached to $H \leq G$. Note that for $H = G$, this recovers the trivial representation. An extremely important special case is $H = 1$, i.e. $X = G$ on which G acts by left multiplication. The resulting permutation representation $K[G]$ is called the *regular representation*. It turns out that the regular representation contains an enormous amount of information about the representation theory of G.

Definition 1.3. A *homomorphism* between representations $\phi : G \to \mathrm{GL}(V)$ and $\psi : G \to \mathrm{GL}(W)$ is a linear map $f : V \to W$ that respects the G-action, i.e. such that for all $g \in G$ and all $v \in V$ one has $f(\phi(g)(v)) = \psi(g)(f(v))$. An isomorphism of representations is a homomorphism that is an isomorphism of vector spaces. If there exists an isomorphism between V and W, then we say that V and W are isomorphic and write $V \cong W$.

Let $\phi : G \to \mathrm{GL}(V)$ be a representation. Once we choose a basis on V, we can express each linear map $V \to V$ as an $n \times n$ matrix with coefficients in K, so that we get a map $G \to \mathrm{GL}_n(K)$, where $\mathrm{GL}_n(K)$ is the group of $n \times n$ invertible matrices with coefficients in K. A homomorphism from

$$\begin{aligned} G &\longrightarrow \mathrm{GL}_n(K),\ g \mapsto X_g \text{ to} \\ G &\longrightarrow \mathrm{GL}_m(K),\ g \mapsto Y_g \end{aligned}$$

is then given by an $n \times m$ matrix A with the property that $AX_g = Y_g A$ for all $g \in G$. An isomorphism is given by such an A that is square and invertible. If we choose a different basis on V, then the matrices X_g all change by conjugation by an invertible matrix. So, as long as we are only interested in representations up to isomorphism, we could define a representation to be a conjugacy class of group homomorphisms $\phi : G \to \mathrm{GL}_n(K)$. Thus, $\phi : G \to \mathrm{GL}_n(K)$ and $\psi : G \to \mathrm{GL}_n(K)$ are considered to be the same representation if there exists $A \in \mathrm{GL}_n(K)$ such that $\phi(g) = A\psi(g)A^{-1}$ for all $g \in G$. This takes care of different choices of basis, as well as of isomorphisms in the sense of Definition 1.3.

1.3 Semi-simplicity and Maschke's theorem

Definition 1.4. A *subrepresentation* of a representation $\phi : G \to \mathrm{GL}(V)$ is a linear subspace U of V that is stable under the G-action, i.e. with the property that $\phi(g)(U) \leq U$ for all $g \in G$.

Exercise 1.5. It is easy to see that if $f : V \to W$ is a homomorphism of representations, then $\ker f = \{v \in V | f(v) = 0\}$ and $\mathrm{Im}\, f = f(V)$ are subrepresentations of V and of W, respectively.

Definition 1.6. A representation is *irreducible* if it has no proper subrepresentations.

Definition 1.7. Given a representation V and a subrepresentation U, the quotient space V/U is naturally a representation via $g(v+U) = gv + U$. This is the *quotient representation*.

Example 1.8. Let G be a finite group and let $K[G]$ be the regular representation over a field K (see Example 1.2 (5)). Recall that a basis of the vector space $K[G]$ is given by $v_g : \ g \in G$. For example, $v = \sum_{g\in G} v_g$ is a vector in $K[G]$. In fact, this vector is invariant under the G-action: for any $h \in G$,

$$h\left(\sum_{g\in G} v_g\right) = \sum_{g\in G} h(v_g) = \sum_{g\in G} (v_{hg}) \overset{g'=hg}{=} \sum_{g'\in G} v_{g'} = v.$$

Thus, the linear span of v is a one-dimensional subrepresentation of $K[G]$, which is isomorphic to the trivial representation. In particular, the regular representation is never irreducible, unless $|G| = 1$.

Definition 1.9. Let V and W be two representations of G. The *direct sum* of V and W is the representation given by the vector space $V \oplus W$ with componentwise G-action, i.e. $g(v, w) = (gv, gw)$.

Exercise 1.10. If V is a representation and U and W are subrepresentations, then it is easy to see, that V is isomorphic to $U \oplus W$ as a representation if and only if it is isomorphic to $U \oplus W$ as a vector space, i.e. if and only if $U + W = V$ and $U \cap W = \{0\}$.

Definition 1.11. A representation is *indecomposable* if it is not a direct sum of proper subrepresentations.

An irreducible representation is certainly indecomposable, but the converse does not always hold (see first exercise sheet). Clearly, to understand all (finite-dimensional) representations of a group over K, it suffices to understand all indecomposable ones, since all representations are direct sums of indecomposable ones. This may be no easy task, however. Irreducibility on the other hand is an extremely restrictive condition and it is often much easier to classify all irreducible representations. But that is not enough to understand all representations. This was the bad news. The good news is that in many situations (and pretty much in all that we will consider here), the two properties – irreducibility and indecomposability – coincide. In other words, every finite dimensional representation is a direct sum of irreducible ones. This is the first big result of the course (do not be deceived by the simplicity of the proof)!

Theorem 1.12 (Maschke's Theorem)**.** *Let G be a finite group and let K be a field of characteristic coprime to $|G|$. Let V be a finite-dimensional representation of G over K and let U be a subrepresentation. Then, there exists a subrepresentation $W \leq V$ such that $V \cong U \oplus W$. We call such a W a* complement *to U in V.*

Proof. Let W' be any complement to U in V as a vector space. Of course, W' need not be a subrepresentation (as an example, think of C_2 acting by reflection on a two-dimensional vector space. The axis of reflection is a subrepresentation and any other line will be a complement of vector spaces. But only the orthogonal line is also a subrepresentation). Out of W', we will construct a

complementary subrepresentation W to U in V as follows: let $\pi' : V \to U$ be the projection along W'. Explicitly, since $V = U \oplus W'$ as vector spaces, we can write each $v \in V$ uniquely as $v = u + w'$, $u \in U$, $w \in W'$, and define $\pi'(v) = u$. Note that π' is not a homomorphism of representations, only of vector spaces. Note also that $\pi'|_U$ is the identity map. Define

$$\pi(v) = \frac{1}{G} \sum_{g \in G} g^{-1} \pi(gv).$$

I claim that $W = \ker \pi$ is the complement we want. Since U is a subrepresentation, $\pi(gu) = gu$ for all $u \in U$, $g \in G$, so that $\pi|_U$ is also the identity map. Thus $W \cap U = \{0\}$. This also shows that π is onto U, so by the rank-nullity formula, $V \cong U \oplus W$ as vector spaces. Finally, it remains to prove that W is a subrepresentation. We do this by showing that π is a homomorphism of representations: given any $v \in V$ and $h \in G$, we have

$$\begin{aligned} \pi(hv) &= \frac{1}{G} \sum_{g \in G} g^{-1} \pi(ghv) \\ &\overset{g' = gh}{=} \frac{1}{G} \sum_{g' \in G} h g'^{-1} \pi(g'v) \\ &= h\pi(v). \end{aligned}$$

So, π is a homomorphism of representations and thus W is a subrepresentation by Exercise 1.5, as required. □

Corollary 1.13. *If G is a finite group and K is a field of characteristic coprime to $|G|$, then any finite-dimensional representation of G over K is a direct sum of irreducible representations.*

Proof. Apply Maschke's theorem inductively. □

This result will have vast consequences, as we shall see soon. But to make proper use of it, we need some more algebraic machinery.

2 Algebras and modules

2.1 Definitions of algebras and modules

A representation is an object with *two* structures that respect each other: it is a vector space, together with a G-action. The G-action is linear, i.e. it respects the vector space structure. It will be convenient to construct an object that "contains" both G and K and that summarises the two actions on V: the scalar multiplication and the G-action.

Definition 2.1. An *algebra* over a field K, or just a K-algebra, is a ring that is also a K-vector space, such that the ring multiplication commutes with scalar multiplication. We will always assume that our algebras contain 1. A *homomorphism* of K-algebras is a K-linear ring homomorphism. A *subalgebra* is a subring that is also a sub-K-vector space.

Example 2.2. 1. The complex numbers form an algebra over $\mathbb{R}$. So do the quaternions (also called Hamiltonians) $\mathbb{H}$. In both cases, $\mathbb{R}$ itself forms a subalgebra. Complex conjugation is an example of a homomorphism $\mathbb{C} \to \mathbb{C}$ of $\mathbb{R}$-algebras.

2. Given any field K and any natural number n, the ring $M_n(K)$ of $n \times n$ matrices with coefficients in K is a K-algebra. The subset of upper triangular matrices forms a subalgebra.

3. The polynomial ring over any field is an algebra.

4. Any K-algebra has a subalgebra isomorphic to K, generated by the identity element. As an exercise, identify this copy of K in all of the above examples.

5. **The following example will be the most important for our purposes**: let G be a finite group. Recall that $K[G]$ is a K-vector space with a canonical basis v_g indexed by the elements of G. To turn it into an algebra, we only need to specify a multiplication operation. Define $v_g \cdot v_h = v_{gh}$ and extend linearly. The resulting algebra is called the *group algebra* of G over K and is also denoted by $K[G]$ (or sometimes KG). We will now stop writing the vectors v_g and will simply write g for the basis elements of the group algebra. Thus, a general element of KG looks like $\sum_{g \in G} a_g g$, $a_g \in K$. To avoid confusion between addition in the vector space and the group operation, we will always denote the group operation of G multiplicatively, even if the group is abelian, unless explicitly otherwise stated.

Definition 2.3. Let M be an abelian group, written additively. The *endomorphism ring* of M, denoted by $\mathrm{End}(M)$, is the ring of homomorphisms from M to itself. Addition is defined using the group operation on M: for $\phi, \psi \in \mathrm{End}(M)$, $(\phi + \psi)(m) = \phi(m) + \psi(m) \in M$; whereas multiplication of endomorphisms is composition of maps $M \to M$: $(\phi \cdot \psi)(m) = \phi(\psi(m))$.

Definition 2.4. Let A be an algebra. A (left) *module* over A, or simply A-module, is an abelian group M together with a ring homomorphism $\phi : A \to \mathrm{End}(M)$. Again, we often write $a(m)$ or $a \cdot m$ or am instead of $\phi(a)(m)$.

Definition 2.5. A *submodule* of an A-module is a subgroup that is stable under the A-action. An A-module is *simple* if it is non-zero and has no proper non-zero submodules. Given an A-module M and a submodule N, the *quotient module* M/N is the quotient group together with the A-action given by $a(mN) = (am)N$.

Definition 2.6. A *homomorphism* $f : M \to N$ between two A-modules is a group homomorphism that commutes with the A-action, i.e. that satisfies $f(a \cdot m) = a \cdot f(m)$.

Definition 2.7. We say that an A-module M is *generated by* $m_i \in M, i \in I$ – an indexing set, and write $M = \langle m_i \mid i \in I \rangle_A$ if

$$\left\{ \sum_{i \in J} a_i m_i \mid J \subseteq I \text{ finite}, a_i \in A \right\} = M.$$

We say that M is *finitely generated* if I can be taken to be finite.

Exercise 2.8. The image $\operatorname{Im} f$ and the kernel $\ker f$ of a homomorphism of modules are submodules of the domain and of the co-domain, respectively.

We have the concept of direct sums, parallel to that of representations:

Definition 2.9. Given A-modules N and N', the direct sum of abelian groups $N \oplus N'$ is an A-module via $a \cdot (n, n') = (a \cdot n, a \cdot n')$. If M is an A-module and N,N' are submodules, then $M \cong N \oplus N'$ if and only if $N + N' = M$ and $N \cap N' = \{0\}$, or equivalently if and only if $M \cong N \oplus N'$ as abelian groups. An A-module is *indecomposable* if it cannot be written as a direct sum of proper submodules.

As for representations, we should think of the irreducible A-modules as those that are usually easier to understand, but not sufficient for understanding all A-modules, while understanding the indecomposable modules is what we really want, but it may be much more difficult.

Proposition 2.10 (First Isomorphism Theorem for modules)**.** *Let A be a K-algebra and let $f : M \to N$ be a homomorphism of A-modules. Then there is an isomorphism $M/\ker(f) \cong \operatorname{Im} f$.*

Proof. The proof is essentially the same as for groups (in fact, we could just refer to the statement for groups and check that everything is compatible with the A-action). Define the map $\bar{f} : M/\ker(f) \to \operatorname{Im} f$ by $\bar{f}(m + \ker(f)) = f(m)$. Check that this is well-defined, i.e. independent of the coset representative m. It is clearly onto the image of f and injective, and it respects the group operations. Since $\ker(f)$ is a submodule, one also checks that $\bar{f}$ is a homomorphism of A-modules, which proves the result. □

Example 2.11.

1. A module over a field is just a vector space. In particular, a module over a K-algebra is automatically a K-vector space. When we talk about the *dimension of a module*, we will always mean dimension over K. A submodule of a K-module is just as sub–vector space. But for a general K-algebra A, a sub–vector space of an A-module will not usually be an A-submodule.

2. An n-dimensional K-vector space is naturally an $M_n(K)$-module.

3. Any algebra acts on itself by left multiplication: $M{=}A$ and for $a \in A$, $m \in M$, $a(m) = am$. This is called the *left regular A-module*. A very important special case of this is $A = M = M_n(K)$. Note that this module is not indecomposable, unless $n = 1$. Indeed, for any $1 \leq i \leq n$, the matrices that are zero outside the i-th column form a submodule.

4. Let V be a K-vector space and $\alpha : V \to V$ any linear map. Let $K[x]$ be the polynomial ring in one indeterminate over K. Then, V can be made into a $K[x]$-module by defining $x \cdot v = \alpha(v)$. A submodule is a vector subspace that is preserved under α.

5. As for modules of group algebras...

Proposition 2.12. *There is a canonical bijection between finite dimensional representations of a finite group G over K and finitely generated non-zero KG-modules. Irreducible representations correspond to simple modules under this bijection.*

Proof. The proof is a straightforward check of the definitions - exercise! □

It may not be clear at this stage what we have gained by reformulating the problem in this way, but it will become clear very soon. The point is that there is a powerful algebraic machinery available to us that investigates the structure of modules over algebras.

2.2 Simple and semi-simple modules, Wedderburn's theorem

Lemma 2.13 (Schur's Lemma)**.** *Let A be a K-algebra and let M and N be two simple A-modules. Then, any A-module homomorphism $M \to N$ is either the 0-map or an isomorphism. If moreover K is algebraically closed, then any isomorphism of simple modules is multiplication by some scalar $\lambda \in K$.*

Proof. Let $f : M \to N$ be a homomorphism of A-modules. Since $\ker f$ is a submodule of M, and since M is simple, $\ker f$ is either 0 or M. If $\ker f = M$, then $f = 0$. Suppose that $f \neq 0$, so f is injective. Since $\operatorname{Im} f$ is a submodule of N, it is either 0 or N by the same argument. Since $f \neq 0$, we have $\operatorname{Im} f \neq 0$, so $\operatorname{Im} f = N$ and thus f is an isomorphism.

Now, let f be an isomorphism. If K is algebraically closed, then f has an eigenvalue, λ, say. But $f - \lambda \cdot \mathrm{id}$ is then also a homomorphism of simple modules and by assumption, it has a kernel. Thus, by the same argument, it is identically 0, so $f = \lambda \cdot \mathrm{id}$. □

Definition 2.14. We say that a module is *semi-simple* if it is a direct sum of simple modules.

In this language, Maschke's theorem says that if G is a finite group and K is a field of characteristic coprime to $|G|$, then every finitely generated non-zero KG-module is semi-simple. In this section, we will explore some of the consequences of this remarkable result.

Note that, among other things, Maschke's theorem says that the left regular module of the group algebra KG itself is semi-simple. Why is this so great? Here is why:

Proposition 2.15. *Let G be a finite group and K a field of characteristic coprime to $|G|$. Then, any simple KG-module is a direct summand of the left regular KG-module.*

Proof. Let M be a simple KG-module. We first define a module homomorphism $f : KG \to M$: let $0 \neq m \in M$ and define

$$f\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g g(m).$$

This is clearly a module homomorphism. Since M is simple and $\operatorname{Im} f \neq 0$ (e.g. $f(1) = m \neq 0$), f must be onto. By the first isomorphism theorem, $M \cong KG/\ker f$. So we have already shown that M occurs as a quotient of the left regular module. But by Maschke's theorem, there exists a submodule N of KG such that $KG = N \oplus \ker f$. Since $KG/\ker f \cong N$, we deduce that $M \cong N \leq KG$. □

To recapitulate: any finitely generated module over an algebra is a direct sum of indecomposable modules. Any *semi-simple* module is a direct sum of simple modules. Usually, there are less of the latter than the former, but in the favourable situation that K has characteristic coprime to $|G|$, all KG-modules are in fact semi-simple. In other words, the notions "indecomposable" and "simple" are the same. Since a general module will be a direct sum of simple summands, we have reduced the problem of understanding all KG-modules to that of understanding the simple ones. But each of those is a direct summand of the left regular module. So all we need to do is decompose the left regular module KG into a direct sum of simple ones and we get the list of *all* simple KG-modules. That latter task is made considerably easier but Wedderburn's theorem, a really big classification result, which we shall not prove here.

Definition 2.16. An algebra is called left (resp. right) *semi-simple* if its left (resp. right) regular module is semi-simple.

Definition 2.17. A division algebra over a field K is a K-algebra in which every element has a multiplicative left and right inverse (the two may be distinct).

Theorem 2.18 (Wedderburn's Theorem)**.** *A K-algebra A is semi-simple if and only if it is isomorphic to a direct sum of matrix algebras over division K-algebras, i.e. if and only if*

$$A \cong \bigoplus_i M_{n_i}(D_i),$$

where $n_i \in \mathbb{N}$ and D_i are division algebras over K.

The proof is slightly technical and beyond the scope of this course. It can be found in many textbooks on algebra, e.g. [1, Theorem 9.5.1].

Remark 2.19.

- Emil Artin has generalised this to semi-simple Artinian rings. The more general result is known as the Artin-Wedderburn theorem.
- The "if" direction of this theorem is actually easy! But the "only if" direction would require two more lectures.
- It is easy to check that each Wedderburn component, treated as a module, decomposes into a direct sum of n mutually isomorphic n-dimensional simple modules. See the first exercise sheet. The simple modules corresponding to different Wedderburn components are certainly not isomorphic, since they have different annihilators.

2.3 Idempotents, more on the group algebra

We now know that given a finite group G and a field K of characteristic coprime to $|G|$, we have an abstract isomorphism of algebras $KG \cong \bigoplus_i M_{n_i}(D_i)$, where D_i are division algebras over K. Moreover, you have shown in the exercises that the left regular module of each $M_{n_i}(D_i)$ is a direct sum of n_i mutually isomorphic simple modules, each of dimension n_i over D_i. An immediate consequence is:

Corollary 2.20. *Let n_i be the dimensions of all the irreducible complex representations of a finite group G. Then $|G| = \sum_i n_i^2$.*

Proof. The only division algebra over $\mathbb{C}$ is $\mathbb{C}$ itself. So $\mathbb{C}G \cong \bigoplus_i M_{n_i}(\mathbb{C})$ and the result follows by comparing dimensions. □

Assumptions 2.21. From now on, we specialise for some time to the case $K = \mathbb{C}$ (or any other algebraically closed field of characteristic 0). We will also always assume that G is finite without explicitly repeating it all the time.

It remains to find a way of explicitly getting a handle on the Wedderburn components $M_{n_i}(\mathbb{C})$, and then we will be able to classify all simple left modules of $\mathbb{C}G$, equivalently all irreducible representations of G over $\mathbb{C}$. Some of the questions that we want to answer are: How many components are there in a given group? How do we explicitly find generators for each of the Wedderburn components in terms of the standard basis on $\mathbb{C}G$? In other words, how do we exhibit each $M_{n_i}(\mathbb{C})$ as a two-sided ideal of $\mathbb{C}G$? The answer will be given in the next section. Here, we prepare the ground.

As a ring, each $M_n(\mathbb{C})$ has a multiplicative identity. Let e_j be the element of $\mathbb{C}G \cong \bigoplus_i M_{n_i}(D_i)$ that has the identity matrix in the j-th entry and zeros elsewhere. Then, e_j is in the centre of $\mathbb{C}G$ and left or right multiplication by e_j is projection onto $M_{n_j}(\mathbb{C})$. We also see that $e_j^2 = e_j$ and that the multiplicative identity of $\mathbb{C}G$ can be written as $1 = \sum_i e_i$.

Definition 2.22. Let R be any ring (e.g. an algebra). An *idempotent* in R is a non-zero element $e \in R$ satisfying $e^2 = e$. A *central idempotent* is an idempotent that is in the centre of the ring. A *primitive central idempotent* is a central idempotent that cannot be written as a sum of two central idempotents. A *complete system of primitive central idempotents* is a set of primitive central idempotents that sum to the identity.

The above discussion shows that the decomposition $\mathbb{C}G \cong \bigoplus_i M_{n_i}(\mathbb{C})$ corresponds to a complete system of primitive central idempotents (the fact that they are primitive is implied by the fact that $M_n(\mathbb{C})$ has no two-sided proper ideals). This is true in complete generality: direct sum decompositions of a ring into proper non-zero two-sided ideals correspond bijectively to decompositions of 1 as a sum of central idempotents. Irreducible ideals (i.e. those without proper two-sided ideals) correspond to primitive idempotents.

Now, each such idempotent can be written as $e = \sum_{g\in G} a_g g$, $a_g \in \mathbb{C}$, and we want to determine a_g, $g \in G$ for all these primitive idempotents.

Example 2.23. Recall that any group has the trivial representation $\mathbf{1} : g \mapsto 1\ \forall g \in G$. In Example 1.8, we have explicitly exhibited the trivial representation as a submodule of the regular module: it is generated by the vector $\sum_{g\in G} g$. However, this element is not idempotent:

$$\left(\sum_{g\in G} g\right)^2 = \sum_{g\in G}\sum_{h\in G} gh = |G| \sum_{g\in G} g.$$

Thus, $e_{\mathbf{1}} = \frac{1}{|G|}\sum_{g\in G} g$ is the primitive central idempotent corresponding to the trivial representation $\mathbf{1}$ of G.

Let $e = \sum_{g\in G} a_g g \in \mathbb{C}G$ be a primitive central idempotent. We begin by determining the coefficient a_1 in terms of the representation ρ that corresponds to e.

Proposition 2.24. *The coefficient a_1 in a primitive central idempotent of $\mathbb{C}G$ corresponding to the Wedderburn block $M_n(\mathbb{C})$ is equal to $\frac{n^2}{|G|}$.*

Proof. Multiplication by e is a linear map on $\mathbb{C}G$. On the Wedderburn component $M_n(\mathbb{C}) = e\mathbb{C}G$ this map acts as the identity, while on the component $(1-e)\mathbb{C}G$ it acts as the zero map. In other words, $\mathbb{C}G = \operatorname{Im} e \oplus \ker e$, and choosing appropriate bases, we see that multiplication by e is given by the matrix $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$, where $\dim \operatorname{Im} e = \operatorname{Tr} e = \dim M_n(\mathbb{C}) = n^2$. Here, $\operatorname{Tr} e$ denotes the trace of the map on $\mathbb{C}G$ given by multiplication by e (recall from linear algebra, that the trace of a matrix is invariant under conjugation, so we can define the trace of a linear map and it is independent of the choice of basis on $\mathbb{C}G$). But also,

$$\operatorname{Tr} e = \sum_{g \in G} a_g \cdot \operatorname{Tr} g.$$

Now, multiplication by $g \neq 1$ correspons to a permutation of the standard basis of $\mathbb{C}G$ without any fixed points, so $\operatorname{Tr} g = 0$ for $g \neq 1$. On the other hand, multiplication by 1 is the identity map on $\mathbb{C}G$, so $\operatorname{Tr} e = a_1 \cdot \operatorname{Tr} 1 = a_1 \cdot |G|$. □

3 Characters

3.1 The first sightings in nature

In the last proposition, it turned out, somewhat unexpectedly, that the traces of matrices might help us to get hold of the primitive central idempotents of a group algebra. This entire section will be about the rôle of traces in our theory. The main outcome of this section will be an explicit description of the idempotents we are after and an amazing almost purely combinatorial procedure that will make calculations of all complex irreducible representations of a given group much easier than the ad hoc methods that you have tried out on the first exercise sheet.

Proposition 3.1. *Let G be a finite group and $\rho : G \to V$ any complex representation. Denote by $V^G = \{v \in V | g(v) = v \ \ \forall g \in G\}$ the fixed subspace under the action of G. In other words, it is the biggest subrepresentation of V that is a direct sum of trivial representations. Then, $V^G = \frac{1}{|G|} \sum_{g \in G} \operatorname{Tr} \rho(g)$.*

Proof. Since V is a direct sum of irreducible representations and since every irreducible representation is a direct summand of the regular representation, we deduce that V is a direct summand of $(\mathbb{C}G)^{\oplus n}$ for some n. We already know that on $\mathbb{C}G$, multiplication by $e_{\mathbf{1}} = \frac{1}{|G|} \sum_{g \in G} g$ is the projection onto the trivial summand of $\mathbb{C}G$. It follows that $V^G = e_{\mathbf{1}} V$. Moreover, choosing a complementary subrepresentation $U \leq V$ such that $V = V^G \oplus U$, as we may by Maschke's theorem, we immediately see that $e_{\mathbf{1}}$ is the identity map on V^G and the zero map on U, and therefore

$$\dim V^G = \operatorname{Tr} \rho(e_{\mathbf{1}}) = \frac{1}{|G|} \sum_{g \in G} \operatorname{Tr} \rho(g),$$

as claimed. □

We are thus led to the following definition:

Definition 3.2. Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation. We define its *character* χ_ρ by $\chi_\rho(g) = \operatorname{Tr} \rho(g)$. This is independent of the choice of basis on V, since $\operatorname{Tr} MAM^{-1} = \operatorname{Tr} A$ for all square matrices A and all invertible M. We call a character *irreducible* if the associated representation is irreducible. The dimension of the representation, which is also the character value at 1, is referred to as the *degree* of the character.

The quantity $\dim V^G$ for a representation of G can be interpreted as the dimension of $\mathrm{Hom}_G(\mathbf{1}, V)$, the space of all homomorphisms of representations between the trivial representation and V. That these two are indeed the same follows from Schur's Lemma. We would now like to find a similar formula for $\dim \mathrm{Hom}_G(V, W)$ for arbitrary representations V and W.

Theorem 3.3. *Given two complex representations V and W of G, the space of G-homomorphisms from V to W is a complex vector space of dimension*

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

Remark 3.4. Notice how the previous proposition is a special case of this theorem, using the fact that the character of the trivial representation is just $\chi_{\mathbf{1}}(g) = 1 \ \forall g \in G$.

Proof. The space of vector space homomorphisms from V to W, $\mathrm{Hom}(V, W)$ is a $\mathbb{C}G$-module as follows: for $g \in G$ and $f : V \to W$ a linear map, define $g(f)(v) = g(f(g^{-1}v))$. By definition,

$$\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G.$$

So, by Proposition 3.1,

$$\dim \mathrm{Hom}_G(V, W) = \frac{1}{|G|} \sum_{g \in G} \chi(g), \tag{3.1}$$

where χ is the character associated with the G-representation $\mathrm{Hom}(V, W)$. So it just remains to compute this character. Let $v_1, \ldots, v_n$ be a basis of V and $w_1, \ldots, w_m$ be a basis of W. Then, $f_{i,j}$ defined by $f_{i,j}(v_k) = \delta_{i,k} w_j$ is a basis of $\mathrm{Hom}(V, W)$, where $\delta_{i,k}$ is the usual Kronecker delta. Now, the trace of $g \in G$ acting on $\mathrm{Hom}(V, W)$ is the sum over all i and j of the coefficient of $f_{i,j}$ in $g(f_{i,j})$. Also, for any $f \in \mathrm{Hom}(V, W)$, the coefficient of $f_{i,j}$ in f is the coefficient of w_j in $f(v_i)$. So, we need to compute the coefficient of w_j in $g(f_{i,j})(v_i) = g(f_{i,j}(g^{-1}v_i))$. Let g be represented by the matrix $(X_{i,j})$ on W with respect to $w_1, \ldots, w_m$ and let g^{-1} be represented by $(Y_{k,l})$ on V with respect to $v_1, \ldots, v_n$. Recall, that $f_{i,j}$ sends v_i to w_j and all other basis vectors to 0, so $f_{i,j}(g^{-1}v_i) = Y_{i,i} w_j$. The coefficient of w_j in $g(f_{i,j})(v_i)$ is therefore $X_{j,j} Y_{i,i}$, and so we see that

$$\chi(g) = \sum_{i,j} X_{j,j} Y_{i,i} = \left(\sum_i Y_{i,i} \right) \left(\sum_j X_{j,j} \right) = \chi_V(g) \chi_W(g^{-1}). \tag{3.2}$$

It remains to relate $\chi_V(g^{-1})$ to $\chi_V(g)$.

Lemma 3.5. *Let $\rho : G \to \mathrm{GL}(V)$ be a complex representation of a finite group G. Then $\rho(g)$ is diagonalisable for any $g \in G$.*

Proof. It suffices to show that the minimal polynomial of $\rho(g)$ splits into linear factors. Now, g has finite order, n, say, so $\rho(g)$ satisfies the polynomial $x^n - 1 = \prod_{i=0}^{n-1} x - \zeta_n^i$, where ζ_n is a fixed primitive n-th root of unity. The minimal polynomial must divide $x^n - 1$, so we are done. □

Corollary 3.6. *Let V be any d-dimensional representation of a finite group and let χ be the associated character. If $g \in G$ has order n, then $\chi(g)$ is a sum of d n-th roots of unity and $\chi(g^{-1}) = \overline{(\chi(g))}$.*

Together with equations (3.1) and (3.2), this finishes the proof of the theorem. □

3.2 The character table, orthogonality relations

In light of Theorem 3.3, another definition naturally suggests itself:

Definition 3.7. Let χ and φ be two characters of a finite group G. The *inner product* of χ and φ is defined as

$$\langle \chi, \varphi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\varphi(g)}$$

It is immediately seen that this is indeed a Hermitian inner product on the vector space of complex functions of G spanned by the irreducible characters, i.e. it is linear in the first variable and satisfies $\langle \chi, \varphi \rangle = \overline{\langle \varphi, \chi \rangle}$. Moreover, it is non-degenerate, as the next result demonstrates:

Proposition 3.8. *Let χ and φ be two irreducible characters. Then*

$$\langle \chi, \varphi \rangle_G = \left\{ \begin{smallmatrix} 1, & \chi = \varphi \\ 0, & otherwise \end{smallmatrix} \right\}.$$

Proof. This is an immediate consequence of Theorem 3.3 together with Schur's lemma. □

This proposition is truly remarkable, because it says that a complex representation is uniquely determined by its character. How so? Let ρ be a complex representation. By Maschke's theorem, we know that it is semi-simple, so let $\rho = \bigoplus_i \rho_i^{n_i}$ be a decomposition of ρ into irreducible summands, where $\rho_i \neq \rho_j$ for $i \neq j$. To determine ρ, it suffices to determine the multiplicities n_i of all the irreducible constituents. The character of ρ can be written as $\chi_\rho = \sum_i n_i \chi_{\rho_i}$. By computing the inner product of χ_ρ with all irreducible characters, we find all n_i, and thus we find ρ. Since it is so amazing, let us say it again: an n-dimensional representation assigns to each group element an $n \times n$ matrix, i.e. n^2 numbers. We replace these n^2 numbers by just one, and this one is enough to determine the representation! A large part of the remaining course will consist of exploring the properties of characters.

Note that since trace is invariant under conjugation of matrices, the character is a function $G \to \mathbb{C}$ that is constant on conjugacy classes of the group, i.e. $\chi(hgh^{-1}) = \chi(g)$ for any character χ of G.

Definition 3.9. A function $f : G \to \mathbb{C}$ that is constant on conjugacy classes is called a *class function*.

The set of class functions on G naturally forms a $\mathbb{C}$-vector space whose dimension is equal to the number of conjugacy classes in G. Any character of G is a class function. Moreover, the inner product of characters can be defined similarly on the entire vector space of class functions. The above proposition says that irreducible characters of G form an orthonormal set with respect to this inner product. In particular, they must be linearly independent. In fact, we will now show that the irreducible characters form an orthonormal basis of the space of all class functions. Along the way, we will finally answer the question: how many isomorphism classes of irreducible complex representations does a finite group have?

Theorem 3.10. *The number of distinct irreducible characters of G is equal to the number of conjugacy classes in G. In particular, the irreducible characters form an orthonormal basis of the space of class functions on G with respect to the inner product of Definition 3.7*

Proof. The idea of the proof is to count the dimension of the centre of the group algebra $\mathbb{C}G$ is two different ways. On the one hand, if we write it in terms of the Wedderburn decomposition

$$\mathbb{C}G \cong \bigoplus_i M_{n_i}\mathbb{C},$$

then it is immediate from general linear algebra that the centre consists of elements that are scalar multiplies of the identity in each Wedderburn component:

$$Z(\mathbb{C}G) = \left\{ \bigoplus_i \lambda_i I_{n_i} \middle| \ \lambda_i \in \mathbb{C} \right\},$$

and so has dimension equal to the number of Wedderburn components, which is also the number of isomorphism classes of irreducible complex representations of G. On the other hand,

$$\sum_{g\in G} a_g g \in Z(\mathbb{C}G) \Leftrightarrow \sum_{g\in G} a_g hgh^{-1} = \sum_{g\in G} a_g g \ \forall h \in G \Leftrightarrow a_{hgh^{-1}} = a_g \ \forall h, g \in G.$$

So, an element $\sum_g a_g g$ of the group algebra is central if and only if the coefficients a_g are constant on conjugacy classes. So, writing $C(G)$ for the set of conjugacy classes,

$$Z(\mathbb{C}G) = \left\{ \sum_{c\in C(G)} \left(a_c \sum_{g\in c} g \right) \middle| \ a_c \in \mathbb{C} \right\},$$

which has dimension $|C(G)|$, and the theorem is proven. □

We see that the inner product of characters is in fact defined for any class functions. The orthogonality of the irreducible characters allows one to easily obtain the decomposition of an arbitrary class function into a linear combination of irreducible characters: if $c = \sum_\chi a_\chi \chi$, then $a_\chi = \langle c, \chi \rangle$. Moreover, the inner product gives a convenient way to check whether a given character is irreducible:

Corollary 3.11. *Let χ be a character. Then, χ is irreducible if and only if $\langle \chi, \chi \rangle = 1$.*

The above theorem suggests organising information about the irreducible complex representations of a finite group in a table.

Definition 3.12. The *character table* of a finite group is a square table, whose columns are labelled by the conjugacy classes of elements and where each row corresponds to an irreducible character of the group, listing its values at the representatives of the conjugacy classes.

The magic of characters is that it is often possible to find all irreducible characters without writing knowing the representations themselves.

Example 3.13. Let $G = S_3$. Recall that in symmetric groups, conjugacy classes are the same as the cycle type classes, so the character table will be a 3×3 matrix. We know that all 1-dimensional characters are lifted from G/G' (see first exercise sheet), which in this case is C_2, so that gives us two out of three rows of the character table:

S_3	1	$(1,2)$	$(1,2,3)$
$\mathbf{1}$	1	1	1
ϵ	1	-1	1
ρ	$?$	$?$	$?$

From Wedderburn's theorem, we know that $|G|$ is equal to the squares of the dimensions of the irreducible characters, so the remaining character has dimension 2. Since the last row must be orthogonal to both the first and the second and since they only differ in the value at $(1,2)$, the last character must be 0 in this column. Finally row orthogonality also gives the last value, and the whole character table is

S_3	1	$(1,2)$	$(1,2,3)$
$\mathbf{1}$	1	1	1
ϵ	1	-1	1
ρ	2	0	-1

Example 3.14. Let $G = G_{20} = \langle a, b |\ a^5 = b^4 = 1, bab^{-1} = a^2 \rangle$. This is a semi-direct product of the cyclic group of order 5 and the cyclic group of order 4, the latter acting faithfully on the former. First, we need to determine the conjugacy classes in G. It is immediately seen that all non-trivial powers of a are conjugate, which gives a conjugacy class of size 4, and that no distinct powers of b are conjugate to each other. This quickly yields 5 conjugacy classes, represented by 1, and by ab^i, $0 \leq i \leq 3$, the last three having size 5. The subgroup generated by a is normal and the quotient is cyclic of order 4. Since $\langle a \rangle$ has no proper subgroups, we deduce that $G' = \langle a \rangle$ and that G has therefore 4 one-dimensional characters. This immediately gives all but one row of the character table:

G_{20}	1	a	ab	ab^2	ab^3
$\mathbf{1}$	1	1	1	1	1
χ_1	1	1	i	-1	$-i$
χ_2	1	1	-1	1	-1
χ_3	1	1	$-i$	-1	i
ψ	$?$	x	y	z	w

Just like in the previous example, we deduce that the degree of the remaining character is 4. By comparing the inner products of ψ with $\mathbf{1}$ and with χ_2, we deduce that $y = -w$. By making the same comparison with χ_1 and χ_3 and taking $y = -w$ into account, we deduce that in fact $y = w = 0$. Again comparing the inner products with $\mathbf{1}$ and with any non-trivial degree one character also yields $z = 0$ and then finally $x = -1$. The complete character table then is

G_{20}	1	a	ab	ab^2	ab^3
$\mathbf{1}$	1	1	1	1	1
χ_1	1	1	i	-1	$-i$
χ_2	1	1	-1	1	-1
χ_3	1	1	$-i$	-1	i
ψ	4	-1	0	0	0

Often, the character table is all one needs to know in practice. But if we want to know the actual matrices, we need to be able to determine the Wedderburn components explicitly. Luckily, this is also made possible by the characters:

Theorem 3.15. *Let $\tau : G \to \mathrm{GL}(V)$ be an irreducible complex representation with character χ. Let $M_n\mathbb{C} = U \leq \mathbb{C}G$ be the corresponding Wedderburn summand of $\mathbb{C}G$ (recall that this means that the $\mathbb{C}G$-module U is isomorphic to a direct sum of $\dim(V)$ copies of V) and let e_χ be the corresponding primitive central idempotent, i.e. $e_\chi\mathbb{C}G = U$. Then, we have*

$$e_\chi = \frac{\dim \tau}{|G|} \sum_{g \in G} \operatorname{Tr} \tau(g^{-1})g = \frac{1}{|G|} \sum_{g \in G} \chi(1)\chi(g^{-1})g.$$

Proof. Write $e_\chi = \sum_{g \in G} a_g g$. Let ρ be the character of the regular representation. Recall that $\rho(1) = |G|$ and $\rho(g) = 0$ for all $g \neq 1$, since multiplication by $g \neq 1$ has no fixed points on the standard basis of $\mathbb{C}G$. Therefore,

$$\rho(g^{-1}e_\chi) = |G|a_g \tag{3.3}$$

for any $g \in G$. On the other hand, we know from Wedderburn's theorem that $\rho = \sum_{\chi_i} \chi_i(1)\chi_i$ with the sum running over all irreducible characters of G. If $i \neq j$, then e_{χ_i} acts as zero on $e_{\chi_j}\mathbb{C}G$ (and therefore so does ge_{χ_i} for any $g \in G$). Otherwise, e_{χ_i} acts as the identity, and so ge_{χ_i} acts as g. In summary, we have

$$\rho(g^{-1}e_\chi) = \sum_{\chi_i} \chi_i(1)\chi_i(g^{-1}e_\chi) = \chi(1)\chi(g^{-1}). \tag{3.4}$$

Equating (3.3) and (3.4), we get the result. □

The example of G_{20} was a little bit more cumbersome than that of S_3. Fortunately, the character table bears a lot more symmetry than we have exploited so far. Another orthogonality relation is extremely useful and would have reduced our work in the case of G_{20} considerably:

Proposition 3.16. *Let $g, h \in G$. Then $\sum_\chi \chi(g)\overline{\chi(h)} = 0$ if g is not conjugate to h, and is equal to $|C_G(g)|$, the order of the centraliser of g in G otherwise.*

Proof. Let $g_1, \dots, g_k$ denote representatives of all the conjugacy classes in G, write $cc(g)$ for the conjugacy class of an element. The orthogonality relation between the irreducible characters can be written as

$$|G|\delta_{\chi,\varphi} = \sum_{g\in G} \chi(g)\overline{\varphi(g)} = \sum_{i=1}^{k} |cc(g_i)|\chi(g_i)\overline{\varphi(g_i)}.$$

The orthogonality relations can be written all at once in matrix notation as follows: let X be the $k \times k$ matrix given be the entries of the character table and let $D = \mathrm{diag}\{|cc(g_1), \dots, |cc(g_k)|\}$. Then, we have

$$|G|I_k = XD\overline{X}^{\mathrm{Tr}},$$

where I_k is the $k \times k$ identity matrix. In other words, $\frac{1}{|G|}D\overline{X}^{\mathrm{Tr}}$ is the right inverse of the matrix X. But the right inverse of a square matrix is also its left inverse, so we have

$$|G|I_k = D\overline{X}^{\mathrm{Tr}}X,$$

which, when spelled out row by row, reads

$$|G|\delta_{i,j} = \sum_{\chi\in \mathrm{Irr}\, G} |cc(g_i)|\overline{\chi(g_i)}\chi(g_j).$$

The result now follows from the orbit-stabiliser theorem. □

In particular, one can read off the sizes of the conjugacy classes of G from the character table.

The character table encodes a lot more group theoretic information. For example, we can extract complete information about the sizes of normal subgroups of G just by looking at the character table:

Proposition 3.17. *Any normal subgroup of G is of the form*

$$N = \{g \in G | \chi_i(g) = \chi_i(1)\ \forall \chi_i \in I \subset \mathrm{Irr}(G)\}$$

for some subset I of the set of irreducible characters of G. Moreover, any such set is indeed a normal subgroup of G.

Proof. On the second exercise sheet, you show that if ρ is a representation of G with character χ, then $\ker\rho = \chi^{-1}(\chi(1))$. Since kernels of group homomorphisms are normal subgroups and since the intersection of two normal subgroups is a normal subgroup, we immediately see that sets of the above form are indeed always normal subgroups of G. Moreover, if N is any normal subgroup, then let I be the set of all irreducible characters of G that are lifted from the quotient G/N (see first exercise sheet). Then, by your results from the first exercise sheet, $N = \cap_{\chi\in I} \ker\chi$ as claimed. □

Example 3.18. Let G be as in Example 3.14. By taking $I = \{\chi_1, \chi_2, \chi_3\}$, we see that $\langle a\rangle$ is a normal subgroup. By taking $I = \{\chi_2\}$, we also see that $\langle a, b^2\rangle$ is normal, and these are all the proper non-trivial normal subgroups.

Corollary 3.19. *A group G is simple if and only if* $\ker\chi = \{1\}$ *for all irreducible characters χ of G.*

It also follows that the character table tells us whether a group is soluble. Indeed, G is soluble if and only if there is a chain of normal subgroups $\{1\} \triangleleft N_2 \triangleleft \ldots \triangleleft N_t = G$ such that each has index a prime power in the next. Since the normal subgroups of a group together with their orders can be read off from the character table, and since the character table of G/N can be read off from that of G, such a chain is detectable through the character table.

We can also recover the centre of the group from the character table.

Definition 3.20. Given a representation ρ of G with character χ, define the centre of ρ by

$$Z(\rho) = Z(\chi) = \{g \in G |\ \rho(g) = \lambda I\}.$$

From the second exercise sheet, we have $Z(\chi) = \{g \in G |\ |\chi(g)| = \chi(1)\}$.

It is easy to see that $Z(\rho)$ is a subgroup of G and the restriction of ρ to Z is isomorphic to $\psi^{\oplus\chi(1)}$ for some 1-dimensional character ψ of $Z(\rho)$.

Lemma 3.21. *Let ρ, χ and $Z(\chi)$ be as above. Then $Z(\chi)/\ker\chi$ is cyclic and is contained in the centre of $G/\ker\chi$. Moreover, if χ is irreducible, then $Z(\chi)/\ker\chi$ is equal to the centre of $G/\ker\chi$.*

Proof. Suppose that $\mathrm{Res}_{G/Z(\rho)}\chi = \chi(1)\psi$ for a linear (i.e. one-dimensional) character ψ of $Z(\chi)$. Clearly, $\ker\chi = \ker\psi$. By the first isomorphism theorem, $Z(\chi)/\ker\chi$ is therefore isomorphic to the image of ψ, which is a finite subgroup of $\mathbb{C}^\times$, hence cyclic. Similarly, $Z(\chi)/\ker\chi \cong \chi(Z(\chi))$ is clearly central in $G/\ker\chi \cong \mathrm{Im}\,\rho$. Conversely, if χ is irreducible and $g\ker\chi$ is central in $G/\ker\chi$, then multiplication by g is an automorphism of ρ, hence it is a scalar multiple of the identity by Schur's lemma. □

Corollary 3.22. *The centre of G is equal to $\bigcap_{\chi\in\mathrm{Irr}(G)} Z(\chi)$.*

Proof. You have already shown on the first exercise sheet that $Z(G) \subseteq Z(\chi)$ for any irreducible character χ. For the reverse inclusion, suppose that $g \in Z(\chi)$ for every irreducible χ. By the previous lemma, we have that $g\ker\chi$ is central in $G/\ker\chi$ for all irreducible χ, so that for any $x \in G$, $gx\ker\chi = xg\ker\chi$, i.e. $gxg^{-1}x^{-1} \in \ker\chi$ for all irreducible χ. But $\bigcap_{\chi\in\mathrm{Irr}(G)}\ker\chi = 1$, so $gxg^{-1}x^{-1} = 1$ for all x, and so g is central. □

Definition 3.23. A character χ is called *faithful* if $\ker\chi = 1$.

4 Integrality of characters, central characters

We have now seen some examples of characters that take non-integer, and even non-rational values. However, the values they take are still very special. To explore this, we need some notions from algebraic number theory.

Definition 4.1. A complex number α is an *algebraic integer* if there exists a monic polynomial $f(x)$ (i.e. with highest power entering with coefficient 1) with integer coefficients such that $f(\alpha) = 0$.

We will list without proof some of the most important properties of algebraic integers.

It might appear as though it can be very hard to prove that something is not an algebraic integer. After all, how can we be sure that there is no suitable polynomial? It turns out that this is very easy:

Lemma 4.2. *Let $f(x)$ be an irreducible monic polynomial over $\mathbb{Q}$. Then its roots are algebraic integers if and only if $f(x) \in \mathbb{Z}$.*

Example 4.3. The following lists algebraic integers, together with polynomials that witness their integrality:

- $\alpha = 5$, $F(x) = x - 5$;
- $\alpha = \sqrt{2}$, $f(x) = x^2 - 2$;
- $\alpha = e^{2\pi i/n}$ $n \in \mathbb{N}$, $f(x) = x^n - 1$;
- $\alpha = \frac{1+\sqrt{5}}{2}$, $f(x) = x^2 - x - 1$.

And here some examples of complex numbers that are not algebraic integers: $1/2$, $\frac{1}{2}e^{2\pi i/n}$ for any $n \in \mathbb{N}$, $\frac{1+\sqrt{3}}{2}$, π, $\log(2)$. The last two do not satisfy *any* polynomial equation with rational coefficients – they are transcendental.

Lemma 4.4. *The only algebraic integers that are in $\mathbb{Q}$ are the usual integers $\mathbb{Z}$.*

Proof. Let $\alpha \in \mathbb{Q}$ be an algebraic integer. Clearly, α satisfies the monic rational polynomial $f(x) = x - \alpha$, and this is clearly irreducible. Hence, the result follows from Lemma 4.2. □

The following is completely non-obvious at first glance:

Theorem 4.5. *The subset of $\mathbb{C}$ consisting of algebraic integers is a ring. In other words, if α and β are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.*

It is not at all obvious how, given polynomials for α and β, to explicitly construct a polynomial that will have $\alpha + \beta$, say, as a root. Instead of such a frontal approach, we will surround the problem from the flanks. The proof will proceed in several intermediate results.

Lemma 4.6. *Let $X = \{\alpha_1, \ldots, \alpha_k\}$ be a finite set of algebraic integers. Then, there exists a ring S with the properties*

1. *$\mathbb{Z} \subseteq S \subset \mathbb{C}$;*
2. *$X \subseteq S$;*
3. *S is finitely generated as a $\mathbb{Z}$-module.*

Proof. The numbers α_i satisfy monic polynomials $f_i \in \mathbb{Z}[X]$ of degrees n_i. Consider the finite set

$$Y = \{\alpha_1^{n_1} \cdots \alpha_k^{n_k} | 0 \leq \alpha_i \leq n_i - 1 \text{ for } 1 \leq i \leq k\},$$

and let S be the set of all $\mathbb{Z}$-linear combinations of elements of Y. Then, all the assertions are clear, except for the claim that S is a ring. By definition, it is closed under addition, we just need to prove that S is closed under multiplication. But that follows immediately from the fact that $\alpha_i^{n_i}$ can be expressed as a $\mathbb{Z}$-linear combination of strictly smaller powers of α_i, using f_i, so *any* power of α_i can be expressed as a $\mathbb{Z}$-linear combination of $1, \ldots, \alpha_i^{n_i - 1}$. □

The following is a rather surprising converse to this Lemma 4.6:

Theorem 4.7. *Let S be a ring with $\mathbb{Z} \leq S \leq \mathbb{C}$, and such that S is finitely generated as a $\mathbb{Z}$-module. Then every element of S is an algebraic integer.*

Proof. Let $Y = \{y_1, \ldots, y_k\} \subseteq S$ be a generating set for Y as a $\mathbb{Z}$-module. Then, for any $s \in S$, we have

$$sy_i = \sum_{j=1}^{k} a_{i,j} y_j, \quad a_{i,j} \in \mathbb{Z}.$$

This can be expressed for all i simultaneously by matrix notation: if $A = (a_{i,j})$ and v is the column vector with entries y_i, $1 \leq i \leq k$, then the above equation says

$$sv = Av,$$

so that s is a root of the polynomial $f(X) = \det(XI - A)$. This is a monic polynomial in $\mathbb{Z}[X]$, which proves that s is an algebraic integer. □

Proof of Theorem 4.5. Let α and β be two algebraic integers. By Lemma 4.6, there exists a ring S with $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$ containigα and β that is finitely generated as a $\mathbb{Z}$-module. Since S is a ring, $\alpha + \beta$ and $\alpha\beta \in S$. By Theorem 4.7, $\alpha + \beta$ and $\alpha\beta$ are algebraic integers, as required. □

Corollary 4.8. *Character values are always algebraic integers.*

Proof. We already know that character values are sums of roots of unity. The latter are algebraic (see Example 4.3) and the algebraic integers are closed under sums, hence the result. □

This result will be very useful for group theoretic applications.

Recall from the first exercise sheet that if ρ is an irreducible representation of G and z is an element of the centre of G, then $\rho(g)$ is a scalar matrix, $\lambda_z I$ for some $\lambda_z \in \mathbb{C}^\times$. More generally, if z is any element of the centre of the group algebra $\mathbb{C}G$, then we also have $\rho(z) = \lambda_z I$ for some $\lambda_z \in \mathbb{C}$. Recall that this follows from Schur's Lemma, since the action of a central element of the algebra on any $\mathbb{C}G$-module gives a module homomorphism. Thus, the character χ of ρ satisfies $\chi(z) = \chi(1)\lambda_z$.

Definition 4.9. Define the *central character* ω_χ attached to χ by

$$\omega_\chi : Z(\mathbb{C}G) \to \mathbb{C}, \quad z \mapsto \lambda_z = \chi(z)/\chi(1).$$

This is easily seen to be an algebra homomorphism.

Recall from the proof of Theorem 3.10 that a basis for $Z(\mathbb{C}G)$ is given by sums $\sum_{g \in cc} g$ over conjugacy classes cc in G. Since ω_χ is an algebra homomorphism, and in particular $\mathbb{C}$-linear, it is determined by its values on a basis of $Z(\mathbb{C}G)$. Let cc be a conjugacy class in G and let $CC = \sum_{g \in cc} g$. We compute

$$\omega_\chi(CC)\chi(1) = \chi(CC) = \sum_{g \in cc} \chi(g) = |cc|\chi(g) \text{ for any } g \in cc,$$

and so

$$\omega_\chi(CC) = \frac{|cc|\chi(g)}{\chi(1)} \text{ for any } g \in cc. \tag{4.5}$$

Since conjugacy class sizes are determined by the character table through column orthogonality, we deduce in particular that central characters are determined by the character table.

Theorem 4.10. *Let χ be an irreducible character of G with associated central character ω_χ. Let CC be a class sum, as before. Then, $\omega_\chi(CC)$ is an algebraic integer.*

Proof. Let $CC_1, \ldots, CC_r$ be the class sums in G. Recall that they constitute a basis for $Z(\mathbb{C}G)$. Thus, we can write

$$CC_iCC_j = \sum_{k=1}^{r} a_{i,j,k} CC_k.$$

I claim that the coefficients are non-negative integers. Indeed, to find the coefficient of one $CC_k = \sum_{g \in cc_k} g$, we only need to look at the coefficient of some $g_k \in cc_k$ in $CC_iCC_j = (\sum_{g \in cc_i} g)(\sum_{h \in cc_j} h)$. But that is just the number of ways of writing g_k as gh, $g \in cc_i$, $h \in cc_j$, and thus a non-negative integer. It follows that the set S of all $\mathbb{Z}$-linear combinations of $\omega_\chi(CC_k)$, $1 \leq k \leq r$, is closed under multiplication and therefore constitutes a ring. Moreover, $\omega_\chi(1) = 1$, so $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$ and Theorem 4.7 applies, showing that all elements of S are algebraic integers, which completes the proof. □

We can now deduce another property of irreducible characters that is very useful for finding character tables:

Theorem 4.11. *Let χ be an irreducible character of the group G. Then $\chi(1) \big| |G|$.*

Proof. By orthonormality of characters, we have

$$|G| = \sum_g \chi(g)\overline{\chi(g)}.$$

We will rewrite this equation in terms of the central character ω_χ. Let $cc_1, \ldots, cc_r$ be the conjugacy classes in G with sums CC_i and representatives g_i. Then, grouping the above sum over the conjugacy classes, we get

$$|G| = \sum_{i=1}^{r} |cc_i|\chi(g)\overline{\chi(g)} = \sum_{i=1}^{r} \chi(1)\omega_\chi(g)\overline{\chi(g)}.$$

So $G/\chi(1) = \sum_{i=1}^{r} \omega_\chi(g)\overline{\chi(g)}$ is an algebraic integer. But also, $G/\chi(1) \in \mathbb{Q}$, so is in fact an integer by Lemma 4.4. □

Using a similar idea, we can prove an even stronger divisibility result:

Theorem 4.12. *Let $\chi \in \mathrm{Irr}(G)$. Then $\chi(1) \big| [G : Z(\chi)]$.*

Proof. We can regard χ as an irreducible character of $G/\ker\chi$ and the statement of the theorem does not change upon passage to that quotient. So, we may without loss of generality assume that $\ker\chi$ is trivial, and therefore $Z(G) = Z(\chi)$. Also, it follows that the associated central character ω_χ is injective on $Z(G)$.

Define an equivalence relation on the elements of G by

$$x \sim y \text{ if for some } z \in Z(G),\ x \text{ is conjugate to } yz.$$

Denote the equivalence classes by $K_1, \ldots, K_s$. I claim that $|\chi(g)|$ is constant on each of these equivalence classes. Indeed, if $x \sim y$, then x is conjugate to yz for some $z \in Z(G)$, so $\chi(x) = \chi(yz)$. But the matrix corresponding to z is a scalar matrix, $\omega_\chi(z)I$, so $\chi(yz) = \chi(y)\omega_\chi(z)$. Moreover, since z has finite order, $|\omega_\chi(z)| = 1$, which proves the claim.

Next, I claim that either χ is 0 on K_i, or else $|K_i| = |cc(g_i)||Z(G)|$, where g_i is any representative of the equivalence class K_i. By definition, every element of K_i is of the form yz for $y \in cc(g_i)$ and $z \in \mathbb{Z}(G)$. So we only need to show that $y_1z_1 = y_2z_2$ for $y_1, y_2 \in cc(g), z_i \in Z(G) \Leftrightarrow y_1 = y_2$ and $z_1 = z_2$. But

$$y_1z_1 = y_2z_2 \Rightarrow \chi(y_1)\omega_\chi(z_1) = \chi(y_1z_1) = \chi(y_2z_2) = \chi(y_2)\omega_\chi(z_2).$$

Moreover, since y_1 is conjugate to y_2, we see that $\chi(y_1) = \chi(y_2)$, and so either $\chi(y_i) = 0$ or $\omega_\chi(z_1) = \omega_\chi(z_2)$. In the latter case, we have $z_1 = z_2$, since ω_χ is injective, whence $y_1 = y_2$, as required. If we pick representatives g_i for the equivalence classes K_i, we now have

$$\begin{aligned} |G| &= \sum_{i=1}^{s} |K_i|\chi(g_i)\overline{\chi(g_i)} \\ &= \sum_{i=1}^{s} |Z(G)||cc(g_i)|\chi(g_i)\overline{\chi(g_i)} \\ &\overset{(4.5)}{=} \sum_{i=1}^{s} |Z(G)|\chi(1)\omega_\chi(CC(g_i))\overline{\chi(g_i)}, \end{aligned}$$

where, as before, $CC(g_i) = \sum_{g \in cc(g_i)} g$. As in the previous proof, we deduce that $|G|/|Z|\chi(1)$ is an algebraic integer, but also a rational number, hence an integer. □

Example 4.13. At this point, we discussed in detail the character tables of $C_2 \wr C_3 \cong (C_2 \times C_2 \times C_2) \rtimes C_3$ and $\mathrm{SL}_2(\mathbb{F}_3) \cong Q_8 \rtimes C_3$.

5 Induced characters

In this section, we will construct representations of a group out of representations of its subgroups. These will in general become reducible, even if the original representation was irreducible, but the construction is still immensely useful for constructing irreducible representations of a group.

Definition 5.1. Let H be a subgroup of a group G and let $\rho : H \to \mathrm{GL}(V)$ be a representation of H. Consider the vector space W of all functions from G to

V satisfying the rule $f(hg) = \rho(h)f(g)$ for all $h \in H$ and $g \in G$. Let G act on W by

$$(g \cdot f)(x) = f(xg).$$

The vector space W with this G-action is the *induction* of ρ to G, written $\mathrm{Ind}_{G/H} \rho$.

Let us begin by finding the dimension of the induced representation. Note that each function f satisfying the above transformation property is uniquely determined by its values on a set of right coset representatives of H in G. It immediately follows that $\dim \mathrm{Ind}_{G/H} \rho = [G : H] \dim \rho$.

Using the above observation that the functions we are interested in are determined by their values on a set of coset representatives, we can give an alternative description of the induced representation. Fix a set $x_1, \ldots, x_r$ of right coset representatives of H in G. This is called a *right transversal* of H in G. Consider the vector space $U = \bigoplus_{i=1}^{r} x_i V$ – a direct sum of $r = [G : H]$ copies of V, indexed by the chosen right transversal. The space W of functions in Definition 5.1 can be identified with U by identifying the function that sends x_i to v_i for $i = 1, \ldots, r$ with the vector $(v_1, \ldots, v_r) \in U = \bigoplus_{i=1}^{r} x_i V$. If we then translate the action of G from the W-language into U-language, then we get the following alternative definition:

Definition 5.2. Let $H \leq G$ and let $\rho : H \to \mathrm{GL}(V)$ be a representation. Choose a right transversal $x_1, \ldots, x_r$ for H in G and define a new vector space $U = \bigoplus_{i=1}^{r} x_i V$ as above. Let G act on U as follows: for $g \in G$, write $x_i g$ uniquely as $h_i x_{n_i}$ for some $n_i \in \{1, \ldots, r\}$ and some $h_i \in H$. For $v = (v_1, \ldots, v_r) \in U$, define $g(v) = (\rho(h_1)v_{n_1}, \ldots, \rho(h_r)v_{n_r})$. Then, U together with this action of G is the induction of ρ to G.

Exercise 5.3. Check that Definition 5.2 of the induced representation is independent of the choice of transversal up to isomorphism, and that it is equivalent to Definition 5.1.

Notice that if we restrict $\mathrm{Ind}_{G/H} \rho$ to H, then we can find a copy of the original representation ρ in the restriction: namely we may, without loss of generality, choose the trivial coset of H in G to be represented by 1, so set $x_1 = 1$ in Definition 5.2. Then, the subspace $x_1 V \oplus 0$ is an H-subrepresentation of $\mathrm{Res}_{G/H} \mathrm{Ind}_{G/H} \rho$ and it is patently isomorphic to ρ itself. In the language of Definition 5.1, this corresponds to the subspace of functions that are 0 outside the trivial coset. Let us record:

Lemma 5.4. *Let $H \leq G$ and let ρ be a representation of H. Then,* $\mathrm{Res}_{G/H} \mathrm{Ind}_{G/H} \rho$ *contains ρ as a direct summand.*

Later, we will greatly generalise this observation.

Example 5.5.

1. Let $\mathbf{1}_H$ be the trivial representation of a subgroup H of G. Then $\mathrm{Ind}_{G/H} \mathbf{1}_H$ is isomorphic to the permutation representation $\mathbb{C}[G/H]$ (see 3rd exercise sheet). In the special case that $H = \{1\}$, this recovers the regular representation of G.

2. Consider $H = C_2 \leq S_3 = G$, let $\tau : H \to \mathrm{GL}(V) = C^\times$ be the non-trivial 1-dimensional representation of C_2. Recall the three irreducible

representations of S_3: $\mathbf{1}$, the sign representation ϵ and a two-dimensional representation ρ. Let us decompose $\mathrm{Ind}_{G/H}\tau$ into irreducibles. First, observe that the restriction of $\mathbf{1}$ to H is the trivial representation, the restriction of ϵ is τ, and the restriction of ρ is a direct sum of the trivial representation and of τ. Since we know that $\mathrm{Res}_{G/H}\mathrm{Ind}_{G/H}\tau$ contains τ as a direct summand, we deduce that $\mathrm{Ind}_{G/H}\tau$ must have at least one of ϵ, ρ in its decomposition into irreducibles. In fact, we can easily show that there must be a summand isomorphic to ρ: the representation $\mathrm{Ind}_{G/H}\tau$ acts on the space $1V \oplus (1,2,3)V \oplus (1,3,2)V$, as described in Definition 5.2. Clearly, 3-cycles act non-trivially on this space, since they permute the summands. But both $\mathbf{1}$ and ϵ are trivial on the 3-cycles, so there must be a copy of ρ in $\mathrm{Ind}_{G/H}\tau$. Since the whole representation is 3-dimensional, the remaining piece is either $\mathbf{1}$ or ϵ. But clearly, the subspace

$$S = \{(v,v,v) | v \in V\} \leq 1V \oplus (1,2,3)V \oplus (1,3,2)V$$

is a subrepresentation that is isomorphic to ϵ (the 3-cycles certainly act trivially, while a 2-cycle contained in H acts through its action on V, which is non-trivial). We deduce that $\mathrm{Ind}_{G/H}\tau \cong \epsilon \oplus \rho$.

To decompose inductions into irreducibles in general, we need to describe the character of an induced representation in terms of the character of the original representation.

Theorem 5.6. *Let χ be the character of a representation $\rho : H \to \mathrm{GL}(V)$, where $H \leq G$. Define the function χ° of G by*

$$\chi^\circ(g) = \begin{cases} \chi(g), & g \in H \\ 0, & \text{otherwise} \end{cases}.$$

Then, the character of the induced representation, written χ^G, is given by

$$\chi^G(g) = \frac{1}{|H|}\sum_{x \in G} \chi^\circ(xgx^{-1}).$$

Proof. The computation will be very similar to the one in the proof of Theorem 3.3. Fix a basis $v_1, \ldots, v_n$ on V and a right transversal $x_1, \ldots, x_r$ of H in G. Then, a basis on W, as defined in Definition 5.1, is given by $f_{i,j} : x_k \mapsto \delta_{i,k} v_j$. For a given $g \in G$, we need to compute the coefficient of $f_{i,j}$ in $g(f_{i,j})$ for all i, j. Now, if $x_i g = h x_j$ for some $i \neq j$, then this coefficient is 0. If, on the other hand, $x_i g = h x_i$ for $h \in H$, i.e. if $x_i g x_i^{-1} \in H$, then the coefficient of $f_{i,j}$ in $g(f_{i,j})$ is equal to the coefficient of v_j in $\rho(h = x_i g x_i^{-1})v_j$. So, we deduce that

$$\begin{aligned} \chi^G(g) &= \sum_{i=1}^{r}\sum_{j=1}^{n} \text{coefficient of } f_{i,j} \text{ in } g(f_{i,j}) \\ &= \sum_{i=1}^{r} \chi^\circ(x_i g x_i^{-1}) \\ &= \sum_{i=1}^{r} \frac{1}{|H|}\sum_{h \in H} \chi^\circ(h x_i g x_i^{-1} h^{-1}) \\ &= \frac{1}{|H|}\sum_{x \in G} \chi^\circ(xgx^{-1}), \end{aligned}$$

as claimed. □

Note that, in particular, if H is normal in G, then $\chi^G(g) = 0$ for $g \notin H$.

Example 5.7. Let $G = S_3$, $H = C_2$, χ the non-trivial one-dimensional character of H, as in Example 5.5. Using the above formula, we see that $\chi^G(1) = 3$, $\chi^G((1,2)) = -1$, $\chi((1,2,3)) = 0$. Taking inner products with the irreducible characters of S_3 confirms the decomposition into irreducibles that we worked out in the previous example.

Note that the formula in Theorem 5.6 makes sense for an arbitrary class function. So we can make the following

Definition 5.8. Let χ be a class function on $H \leq G$. Define the induced class function χ^G on G by

$$\chi^G(g) = \frac{1}{|H|} \sum_{x \in G} \chi^\circ(xgx^{-1}),$$

where χ° is defined by

$$\chi^\circ(g) = \begin{cases} \chi(g), & g \in H \\ 0, & \text{otherwise} \end{cases}.$$

The definitions of induction of representations and of characters may look slightly artificial, but turn out to be "the right ones" in the following sense:

Theorem 5.9 (Frobenius Reciprocity)**.** *Let $H \leq G$, let χ be a class function of H and ϕ a class function of G. Then*

$$\langle \chi^G, \phi \rangle_G = \langle \chi, \phi_G \rangle_H,$$

where ϕ_G denotes the restriction of ϕ to H.

Proof. With the explicit formula for inductions at our disposal, the proof is just a formal computation and I suggest you try it yourself before reading further. So here goes:

$$\begin{aligned}
\langle \chi^G, \phi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi^G(g) \overline{\phi(g)} \\
&= \frac{1}{|G|} \frac{1}{|H|} \sum_{g \in G} \sum_{x \in G} \chi^\circ(xgx^{-1}) \overline{\phi(g)} \\
&\overset{y = xgx^{-1}}{=} \frac{1}{|G|} \frac{1}{|H|} \sum_{x \in G} \sum_{y \in G} \chi^\circ(y) \overline{\phi(x^{-1}yx)} \\
&\overset{\phi(x^{-1}yx) = \phi(y)}{=} \frac{1}{|H|} \sum_{y \in H} \chi(y) \overline{\phi(y)} \\
&= \langle \chi_G, \phi \rangle_H.
\end{aligned}$$

□

Example 5.10. With Frobenius reciprocity, decomposing τ^G of Example 5.5 into irreducibles becomes even easier: we remarked already in that example that the restriction of the trivial representation of S_3 to C_2 is trivial, while the restrictions of the other two irreducible S_3-representations have one copy of τ each as a direct summand. Frobenius reciprocity then says that the representations that enter into τ^G are precisely those that have at least one copy of τ upon restriction to C_2, which confirms our calculations.

Corollary 5.11. *Let H be any subgroup of G. Any irreducible representation of G is a constituent of some induced representation from H.*

Proof. Let ρ be an irreducible representation of G, let τ be a direct summand of $\mathrm{Res}_{G/H}(\rho)$. By Frobenius reciprocity, $\langle \chi_\tau^G, \chi_\rho \rangle > 0$, as required. □

Corollary 5.12. *For $H \leq G$, any irreducible representation of H is a summand of some restriction from G.*

Corollary 5.13. *If G is abelian and $H \leq G$, then any irreducible representation of H is the restriction of some irreducible representation of H.*

Proposition 5.14. *Let χ be a character of $H \leq G$. Choose a set of representatives $x_1, \ldots, x_m$ of conjugacy class representatives of H that are G-conjugate to g. Then*

$$\chi^G(g) = |C_G(g)| \sum_{i=1}^{m} \frac{\chi(x_i)}{|C_H(x_i)|}.$$

Proof. We will begin with the formula of Theorem 5.6:

$$\chi^G(g) = \frac{1}{|H|} \sum_{x \in G} \chi^\circ(xgx^{-1}),$$

where χ° is χ on H and 0 outside H. We can rewrite that as

$$\begin{aligned} \chi^G(g) &= \frac{|C_G(g)|}{|H|} \sum_{\tilde{x} \in cc_G(g)} \chi^\circ(\tilde{x}) = \frac{|C_G(g)|}{|H|} \sum_{i=1}^{m} \sum_{h \in cc_H(x_i)} \chi(h) \\ &= \frac{|C_G(g)|}{|H|} \sum_{i=1}^{m} |cc_H(x_i)| \chi(h) = |C_G(g)| \sum_{i=1}^{m} \frac{\chi(x_i)}{|C_H(x_i)|}, \end{aligned}$$

where the third equality follows from the fact that χ is a class function on H, and the last equality follows from the orbit–stabiliser theorem. □

We will now begin explaining one of the ways in which induced characters are useful for producing irreducible characters.

Lemma 5.15. *Let Ω be a G-set, i.e. G acts on Ω by permuting the elements. Suppose that G acts transitively on Ω. For $\omega \in \Omega$, let*

$$G_\omega = \{g \in G : \ g(\omega) = \omega\}$$

be the point stabiliser. Then the G-set Ω is isomorphic to the G-set G/G_ω – the set of left cosets.

Proof. The isomorphism is given by $gG_\omega \mapsto g(\omega)$. Check that this is well-defined, bijective, and respects the G-action. □

Let χ be the permutation character coming from the G-action on a set Ω. Recall from the second exercise sheet that $\chi(g) = \Omega^g$, and that $\langle \chi, \mathbf{1} \rangle$ is the number of orbits of G on Ω.

Proposition 5.16. *Let Ω be a transitive G-set and let G_ω be a point stabiliser. If χ is the permutation character of Ω, then $\langle \chi, \chi \rangle$ is the number of orbits of G_ω on Ω.*

Proof. Let r be the number of orbits of G_ω on Ω. Then we have

$$r = \langle \chi_{G_\omega}, \mathbf{1}_{G_\omega} \rangle \overset{5.9}{=} \langle \chi, (\mathbf{1}_{G_\omega})^G \rangle \overset{5.15}{=} \langle \chi, \chi \rangle.$$

□

Corollary 5.17. *Let G act doubly-transitively on Ω, meaning that any point stabiliser G_ω acts transitively on $\Omega \backslash \{\omega\}$. If χ is the corresponding permutation character, then $\chi - \mathbf{1}$ is an irreducible character of G.*

Example 5.18. The natural action of S_n on $\{1, \ldots, n\}$ is doubly-transitive when $n \geq 2$, so the above result implies that S_n always has an (easy to compute!) irreducible character of dimension $n - 1$. The same goes for A_n when $n \geq 4$.

6 Some group theoretic applications

6.1 Frobenius groups

Definition 6.1. A non-trivial subgroup H of G is called a *Frobenius complement* if $H \cap gHg^{-1} = \{1\}$ for all $g \in G \backslash H$. A group that has a Frobenius complement is called a *Frobenius group*.

We will prove that if $H \leq G$ is a Frobenius complement, then there exists a normal subgroup $N \triangleleft G$ such that G is a semidirect product of N and H. Recall that $G = N \rtimes H$ if and only if H is a subgroup of G, N is a normal subgroup of G, $G = NH$, and $N \cap H = \{1\}$. Finding a *subset* N with this property is a triviality:

Definition 6.2. Let $H \leq G$ be a Frobenius complement. Define the corresponding *Frobenius kernel* by

$$N = \left(G \backslash \bigcup_{x \in G} H^x \right) \cup \{1\}.$$

The difficult part is to show that this is indeed a normal subgroup. A priori, it is not even obvious that this is a subgroup at all. The original proof of this fact is due to Frobenius and, remarkably, uses character theory. Even more remarkably, more than a 100 years later, there is still no proof available that doesn't use character theory! Before we prove the theorem, let us convince ourselves that if N really is a normal subgroup, then G will be a semi-direct product of N and H.

Lemma 6.3. *With N defined as above, we have $|N| = |G|/|H|$. Moreover, if M is any normal subgroup of G that intersects H trivially, then $M \subseteq N$.*

Proof. Since $H \cap gHg^{-1} = \{1\}$ for all $g \notin H$, there are $[G : H]$ conjugates of H in G and their union contains $[G : H](|H| - 1) = |G|(1 - \frac{1}{|H|})$ non-trivial elements, so $|N| = |G|/|H|$.

If M is a normal subgroup that intersects H trivially, then $M \cap gHg^{-1} = g(g^{-1}Mg \cap H)g^{-1} = g(M \cap H)g^{-1}$ is also trivial for any $g \in G$, so M is contained in N as claimed. □

Let us now marvel at the proof of Frobenius from 1901. We begin with an easy auxiliary result:

Lemma 6.4. *Let $H \leq G$ be a Frobenius complement and let θ be a class function of H that satisfies $\theta(1) = 0$. Then $(\theta^G)_H = \theta$.*

Proof. For any $h \in H$, we have by definition

$$\theta^G(h) = \frac{1}{|H|} \sum_{x \in G} \theta^\circ(xhx^{-1}).$$

If $h = 1$, this is still 0. So let $h \in H$ be non-trivial. Now, $\theta^\circ(xhx^{-1}) \in xHx^{-1}$. But also, this term is only non-zero if $xhx^{-1} \in H$. But since H is a Frobenius complement, $xhx^{-1} \in H \cap xHx^{-1}$ implies that $x \in H$. Since θ is a class function, we then have $\theta^\circ(xhx^{-1}) = \theta(h)$, so that

$$\theta^G(h) = \frac{1}{|H|} \sum_{x \in H} \theta(h) = \theta(h),$$

as claimed. □

Theorem 6.5. *Let $H \leq G$ be a Frobenius complement. The corresponding Frobenius kernel N is a normal subgroup of G and $G = N \rtimes H$.*

Proof. Roughly, the strategy of the proof will be to show that we can extend any character of H to a character of G. This is to be expected if H is supposed to be isomorphic to a quotient of G.

Let ϕ be a non-trivial irreducible character of H, define the class function $\theta = \phi - \phi(1)\mathbf{1}_H$. So, $\theta(1) = 0$ and satisfies the hypothesis of the previous lemma. We therefore have, using Frobenius reciprocity

$$\langle \theta^G, \theta^G \rangle_G = \langle \theta, (\theta^G)_H \rangle_H = \langle \theta, \theta \rangle_H = 1 + \phi(1)^2.$$

Also, using Frobenius reciprocity again, we have

$$\langle \theta^G, \mathbf{1}_G \rangle_G = \langle \theta, \mathbf{1}_H \rangle_H = -\phi(1),$$

so it is natural to consider the class function $\tilde{\phi} = \theta^G + \phi(1)\mathbf{1}_G$. We have $\langle \tilde{\phi}, \mathbf{1}_G \rangle_G = 0$ and

$$\langle \tilde{\phi}, \tilde{\phi} \rangle = \langle \theta^G + \phi(1)\mathbf{1}, \theta^G + \phi(1)\mathbf{1} \rangle = \langle \theta^G, \theta^G \rangle + 2\phi(1)\langle \theta^G, \mathbf{1} \rangle + \phi(1)^2 \langle \mathbf{1}, \mathbf{1} \rangle = 1.$$

Since $\tilde{\phi}$ is not just a class function, but a difference of characters, we deduce that either $\tilde{\phi}$ or $-\tilde{\phi}$ is an irreducible character. We can easily determine which is the case: if $h \in H$, then

$$\tilde{\phi}(h) = \theta^G(h) + \phi(1) = \theta(h) + \phi(1) = \phi(h).$$

In particular, $\tilde{\phi}(1) = \phi(1) > 0$, so $\tilde{\phi}$ is an irreducible character. We have therefore extended each non-trivial $\phi \in \mathrm{Irr}(G)$ to the whole of G. Define

$$M = \bigcap_{\phi} \ker(\tilde{\phi}).$$

We first show that M satisfies the hypothesis of Lemma 6.3. If $h \in M \cap H$, then for any $\phi \in \mathrm{Irr}(H)$, $\phi(h) = \tilde{\phi}(h) = \tilde{\phi}(1) = \phi(1)$, i.e. $M \cap H = \bigcap_{\phi \in \mathrm{Irr}(H)} \ker(\phi) = \{1\}$. It thus follows by Lemma 6.3 that $M \subset N$ and it remains to prove the opposite inclusion. Let $g \in G$ be not contained in any conjugate of H, equivalently suppose that no conjugate of g lies in H. Then, for any $\phi \in \mathrm{Irr}(H)$,

$$\tilde{\phi}(g) - \phi(1) = \theta^G(g) = 0,$$

so $g \in \ker \tilde{\phi}$. Thus $N = M$ is a normal subgroup, as claimed. Moreover, $N \cap H = \{1\}$ and we already know that $|N| = |G|/|H|$, which implies that $NH = G$. □

6.2 Burnside's $p^\alpha q^\beta$-theorem

Our next group theoretic application will be a result on finite simple groups. It will give you a very small idea of how pivotal representation theory has been in the classification of finite simple groups. As usual, we need some preparation. All of the results in this subsection are due to William Burnside.

Theorem 6.6. *Let $\chi \in \mathrm{Irr}(G)$ and let CC be a conjugacy class of G of size coprime to $\chi(1)$. Then for any $g \in CC$, either $g \in Z(\chi)$ or $\chi(g) = 0$.*

Proof. Recall that $\frac{\chi(g)|CC|}{\chi(1)}$ is an algebraic integer. Since $(\chi(1), |CC|) = 1$, there exist integers u, v such that

$$u\chi(1) + v|CC| = 1.$$

We therefore have that

$$\frac{\chi(g)}{\chi(1)} - u\chi(g) = \frac{\chi(g)(1 - u\chi(1))}{\chi(1)} = v\frac{\chi(g)|CC|}{\chi(1)}$$

is also an algebraic integer. Since $u\chi(g)$ is an algebraic integer, we deduce that so is $\alpha = \chi(g)/\chi(1)$. Recall that if the order of g is n, then $\chi(g)$ is a sum of $\chi(1)$ n-th roots of unity, so that $|\chi(g)| \leq \chi(1)$ with equality if and only if $g \in Z(\chi)$. Now, α is an element of the field

$$\mathbb{Q}(\zeta) = \left\{ \sum_{i=0}^{n-1} x_i \zeta^i \Big| \; x_i \in \mathbb{Q} \right\},$$

where $\zeta = e^{2\pi i/n}$. It is a fact in algebraic number theory that the algebraic integers in $\mathbb{Q}(\zeta)$ are precisely those elements, for which the coefficients x_i are in $\mathbb{Z}$. It follows that if $\alpha = \left(\sum_{i=1}^{\chi(1)} \zeta^{k_i}\right)/\chi(1)$ is an algebraic integer, then either k_i are equal for all $i \in \{1, \ldots, \chi(1)\}$, or $\alpha = 0$. This proves the result. □

Theorem 6.7. *If a non-trivial conjugacy class of a simple group G has prime power size, then G is cyclic.*

Proof. Suppose that G is simple and non-abelian and that $g \in G$ has conjugacy class CC of size $p^\alpha > 1$, where p is a prime number. Let χ be a non-trivial irreducible character of G. By simplicity, $\ker \chi = \{1\}$ and $Z(\chi) = Z(G) = \{1\}$. By the previous theorem, either $p|\chi(1)$ or $\chi(g) = 0$. By column orthogonality, we then have

$$0 = \sum_{\chi \in \operatorname{Irr} G} \chi(1)\chi(g) = 1 + \sum_{\chi:\, p|\chi(1)} \chi(1)\chi(g),$$

so $-1/p = \sum \frac{\chi(1)}{p}\chi(g)$. But the right hand side is an algebraic integer, while the left hand side clearly isn't, which gives a contradiction. □

Theorem 6.8. *A group of size $p^\alpha q^\beta$ with p, q prime is soluble.*

Proof. If either α or β is 0, then this is elementary group theory. So take $\alpha, \beta > 0$, $p \neq q$. Let G be a minimal counterexample to the assertion. If N is any non-trivial proper normal subgroup, then both N and G/N are soluble by minimality of G. So such a counterexample must be simple (and of course non-abelian). Let P be a Sylow p-subgroup of G. It has non-trivial centre, so choose $1 \neq g \in Z(P)$, so that $C_G(g)$ contains P. Then $|CC(g)| = |G|/|C_G(g)|$ is a power of q, which contradicts the previous theorem. □

7 Advanced topics on induction and restriction

7.1 Mackey decomposition and Mackey's irreducibility criterion

A natural question is: what happens to a representation ρ of $H \leq G$ after we induce it to G and restrict it back to H. It's dimension goes up, and we already know that ρ is a direct summand of the resulting representations. Thus, it cannot be irreducible, even if ρ is. We would like to be able to decompose the resulting representation of H into (ideally irreducible) summands. We will consider an even more general situation, where the group that we are inducing from need not be the same as the one we are restricting to.

For preparation, we need to recall the concept of double cosets. Let H and K be subgroups of a group G. Given $g \in G$, the double coset KgH is

$$KgH = \{kgh : \ h \in H, k \in K\}.$$

Clearly,

$$\begin{aligned} KgH = Kg'H \quad &\Leftrightarrow \quad kgh = k'g'h' \text{ for some } h, h' \in H,\ k, k' \in K \\ &\Leftrightarrow \quad g = k^{-1}k'g'h'h^{-1} \\ &\Leftrightarrow \quad g \in Kg'H. \end{aligned}$$

It easily follows that being in the same double coset is an equivalence relation, and that double cosets partition the group. The set of double cosets is denoted by $K\backslash G/H$. We will often write $g \in K\backslash G/H$ instead of $KgH \in K\backslash G/H$, i.e. in that notation g will mean a double coset representative.

Unfortunately, double cosets are not nearly as well-behaved as usual cosets. E.g. they need not be of the same size, nor does their size always divide the order of the group.

Example 7.1. Let $G = S_3$, $H = K = \langle (1,2) \rangle$. Clearly, the trivial coset $K1H$ consists only of H itself. Further,

$$\begin{aligned} H(1,3)K &= \{(1,3), (1,2)(1,3), (1,3)(1,2), (1,2)(1,3)(1,2)\} \\ &= \{(1,3), (1,2,3), (1,3,2), (2,3)\}. \end{aligned}$$

So we see that $G = K1H \cup K(1,2)H$ and the two double cosets have orders 2 and 4, respectively.

Theorem 7.2 (Mackey's Decomposition Theorem)**.** *Let H, K be subgroups of G and let $\rho : K \to \mathrm{GL}(V)$ be a representation of K. Then*

$$\mathrm{Res}_{G/H} \mathrm{Ind}_{G/K}(\rho) = \bigoplus_{g \in K\backslash G/H} \mathrm{Ind}_{H/H\cap K^g} \mathrm{Res}_{K^g/H\cap K^g}(\rho^g),$$

where $K^g = gKg^{-1}$ and ρ^g is the representation of K^g defined by $\rho^g(gkg^{-1}) = \rho(k)$.

Proof. Recall that the vector space of ρ^G is $\oplus_i x_i V$, where $x_1, \ldots, x_r$ is a set of right coset representatives of K in G. If for some $h \in H$, $x_i h = k x_j$, then $x_i \in K x_j H$. Thus, for any j, the subspace

$$\bigoplus_{x_i \in K x_j H} x_i V$$

is an H-subrepresentation of $\mathrm{Ind}_{G/K} \rho$, and it remains to prove that it is isomorphic to $\mathrm{Ind}_{H/H\cap K^{x_j}} \mathrm{Res}_{K^{x_j}/H\cap K^{x_j}}(\rho^{x_j})$. Fix $x = x_j$. One immediately sees that $x^{-1}kx$ acts on xV through $\mathrm{Res}_{K^x/H\cap K^x}(\rho^x)$. Also, for each $x_i \in KxH$, write $x = k_i x_i h_i$, so that $x_i^{-1} k_i^{-1} x = h_i \in H$. Then, the assignment $x_i \mapsto x_i^{-1} k_i^{-1} x$ induces a bijection between the coset representatives of $K\backslash G$ that lie in the double coset KxH and the coset representatives of $(K^x \cap H)\backslash H$. The claim now follows. □

We have already observed several times that the induction of a representation is rarely irreducible, even if the original representation is. On the fourth exercise sheet, you will see an important instance of induced representations that *are* irreducible. The following result may sometimes help detect this favourable situation:

Theorem 7.3 (Mackey's irreducibility criterion)**.** *Let $H \leq G$ and let $\rho : H \to \mathrm{GL}(V)$ be a representation. Then, $\mathrm{Ind}_{G/H} \rho$ is irreducible if and only if the following two conditions are satisfied:*

1. *ρ is irreducible, and*
2. *for any $g \in G\backslash H$, the two representations $\mathrm{Res}_{H^g\cap H} \rho$ and $\mathrm{Res}_{H^g\cap H} \rho^g$ have no irreducible summand in common, i.e. if the inner product of the associated characters is 0.*

Proof. Let χ be the character of ρ. The character χ^G is irreducible if and only if $\langle \chi^G, \chi^G \rangle_G = 1$. Using Frobenius reciprocity twice and Mackey's decomposition theorem, we get

$$\begin{aligned} \langle \chi^G, \chi^G \rangle_G = \langle \chi, (\chi^G)_H \rangle_H &= \langle \chi, \sum_{g \in H\backslash G/H} \mathrm{Res}_{H^g \cap H}(\chi^g)^H \rangle_H \\ &= \sum_{g \in H\backslash G/H} \langle \mathrm{Res}_{H^g \cap H}(\chi), \mathrm{Res}_{H^g \cap H}(\chi^g) \rangle_{H^g \cap H}. \end{aligned}$$

In the last sum, the summand corresponding to $g = 1$ is at least equal to 1 and all other summands are non-negative. So χ^G is irreducible if and only if $\langle \chi, \chi \rangle = 1$ and all other summands are equal to 0, as claimed. □

7.2 Restriction to and induction from normal subgroups

Let N be a normal subgroup of G. Then, G acts on the space of class functions of N via $\tau^g(n) = \tau(g^{-1}ng)$ where τ is any class function of N, $g \in G$, and $n \in N$. Clearly, this action sends irreducible characters to irreducible characters. More generally, $\langle \tau_1, \tau_2 \rangle = \langle \tau_1^g, \tau_2^g \rangle$ for any class functions τ_1, τ_2 of N and any $g \in G$. We call two class functions of N that lie in the same G-orbit *G-conjugate*.

Theorem 7.4 (Clifford's Theorem)**.** *Let χ be an irreducible character of G and let $N \triangleleft G$. Then $\mathrm{Res}_{G/N} \chi = e(\tau_1 + \ldots + \tau_t)$ for some $e \in \mathbb{N}$, where the $\tau_i \in \mathrm{Irr}(N)$ form one orbit under the action of G.*

Proof. Let $\tau = \tau_1$ be an irreducible constituent of $\chi_N = \mathrm{Res}_{G/N} \chi$ with multiplicity e. Since χ is a class function of G, $\chi^g(h) = \chi(ghg^{-1}) = \chi(h)$ and it follows immediately that

$$\langle \tau, \chi_N \rangle_N = \langle \tau^G, \chi \rangle_G = \langle (\tau^G)^g, \chi^g \rangle_G = \langle (\tau^g)^G, \chi \rangle_G = \langle \tau^g, \chi_N \rangle_N,$$

so that any G-conjugate of τ is also a constituent of G with multiplicity e. It remains to show that any constituent of χ_N is G-conjugate to τ. Let ψ be an irreducible consituent of χ_N. By Frobenius reciprocity, we then have $\langle \chi, \psi^G \rangle > 0$, so that $\psi^G = \chi + \ldots$, and so $(\psi^G)_N = \chi_N + \ldots$, thus $\langle (\psi^G)_N, \tau_1 \rangle > 0$. So, applying the Mackey decomposition formula, we have $\langle \sum_{N\backslash G/N} (\psi^g)^N_{N \cap N^g}, \tau_1 \rangle > 0$. But N is normal, so this gives $\sum_{N\backslash G/N} \langle \psi^g, \tau_1 \rangle > 0$. Since all the characters involved are irreducible, this implies that $\psi^g = \tau_1$ for some $g \in G$. □

This result has some strong and interesting consequences.

Corollary 7.5. *Let $N \triangleleft G$ and let $\chi \in \mathrm{Irr}(G)$ be such that $\langle \chi_N, \mathbf{1} \rangle_N \neq 0$. Then, $N \subset \ker \chi$.*

Proof. Clearly, $\mathbf{1}_H$ consitutes a single orbit in $\mathrm{Irr}(N)$ under the G-action, so the result follows immediately from the previous theorem. □

Corollary 7.6. *Let $N \triangleleft G$, let $\chi \in \mathrm{Irr}(G)$ and $\phi \in \mathrm{Irr}(N)$ be such that $\langle \chi_N, \phi \rangle_N \neq 0$. Then, $\phi(1) | \chi(1)$.*

Proof. Clearly, $\phi^g(1) = \phi(1)$ for any $\phi \in \mathrm{Irr}(N)$ and any $g \in G$. So, the result follows immediately from Theorem 7.4 □

Here, we have only scratched the surface of the interesting interplay between characters of G and characters of a normal subgroup of G. For much more on this topic, see e.g. [2, Ch. 6].

7.3 Base fields other than $\mathbb{C}$

We will briefly state without proof how the results of this section generalise to representations over arbitrary fields.

Note that the definition of the induced representation makes perfect sense over any field. So does the statement of Mackey's formula. Moreover, since the only thing we used in the proof of Mackey's formula was the definition of induced representations, that proof remains valid over any field. On the other hand, Frobenius reciprocity is phrased in terms of characters, so does not immediately say anything about irreducible representations over arbitrary fields. However, it can be phrased purely in terms of representations and is then valid over any field:

Theorem 7.7. *Given a subgroup H of G, a $K[H]$-module V and a $K[G]$-module W, we have*

$$\mathrm{Hom}_{K[G]}(\mathrm{Ind}_{G/H} V, W) \cong \mathrm{Hom}_{K[H]}(V, \mathrm{Res}_{G/H} W).$$

Clifford's theorem also makes sense and is true over any field.

8 Real representations, duals, tensor products, Frobenius-Schur indicators

8.1 Dual representation

Let V be a vector space over an arbitrary field K. Recall that the dual vector space is defined by

$$V^* = \{f : V \to K : f(v + \alpha w) = f(v) + \alpha f(w)\}.$$

Definition 8.1. If $\rho : G \to \mathrm{GL}(V)$ is a representation over K, then the *dual representation* $\rho^* : G \to \mathrm{GL}(V^*)$ is defined by

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

The inverse is necessary to get a left action, and you should check that this really does give a left action.

Let fix a basis $v_1, \ldots, v_n$ be a basis of V. Recall that the dual basis $f_1, \ldots, f_n$ is given by $f_i(v_j) = \delta_{i,j}$. Suppose that $\rho(g^{-1})$ is given by the matrix $A = (a_{i,j})$ with respect to $v_1, \ldots, v_n$. Then

$$\rho^*(g)(f_i)(v_j) = f_i(Av_j) = f_i(\sum_k a_{j,k} v_k) = a_{j,i}.$$

So the matrix of $\rho^*(g)$ with respect to the dual basis is A^{Tr}.

In particular, we deduce that if $K = \mathbb{C}$ and χ is the character of ρ, then the character χ^* of ρ^* is

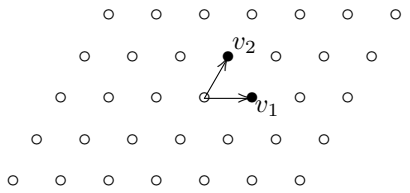
$$\chi^*(g) = \overline{\chi(g)}.$$

Corollary 8.2. *A complex representation is isomorphic to its own dual (we say that it is* self-dual*) if and only if its character is real-valued.*

This raises a natural question: given a complex representation $\rho : G \to \mathrm{GL}(V)$, when can we choose a basis on V, such that all group elements are represented by real matrices? Clearly, the character being real-valued is a necessary condition. To find necessary and sufficient conditions will be the main theme of this section.

Definition 8.3. Let $\rho : G \to \mathrm{GL}(V)$ be a representation over a field K and let F be a subfield of K. We say that ρ is realisable over F if there exists a basis of V with respect to which all elements of g are represented by matrices with coefficients in F.

Example 8.4. Let $G = S_3 \cong D_6$, let ρ be the irreducible comple two-dimensional representation of G. Recall that the 3-cycles in S_3 act by rotation by $2\pi/3$ under ρ. The usual rotation matrix for counter-clockwise rotation by $2\pi/3$ is $\begin{pmatrix} \cos 2\pi/3 & \sin 2\pi/3 \\ -\sin 2\pi/3 & \cos 2\pi/3 \end{pmatrix}$. However, choosing a judicious basis on our vector space, as in the picture, we can make the matrix corresponding to such a rotation look like $\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$.



Thus, ρ is realisable over $\mathbb{Q}$.

Recall that an homomorphism of vector spaces $\iota : V \to V^*$ gives rise to a bilinear pairing

$$\begin{aligned} \langle \_, \_ \rangle &: V \times V \to K \\ \langle v, w \rangle &= \iota(v)(w). \end{aligned}$$

Conversely, given a bilinear pairing as above, one gets a homomorphism $V \to V^*$ by $v \mapsto \langle v, \_ \rangle = (w \mapsto \langle v, w \rangle)$. The map ι is an isomorphism of vector spaces if and only if the associated pairing is non-degenerate. Also, it is easy to see that ι is an isomorphism of G-representations if and only if the associated pairing is G-invariant, i.e. if and only if

$$\langle gv, gw \rangle = \langle v, w \rangle \ \forall g \in G, v \in V, w \in W.$$

Theorem 8.5. *Let $\rho : G \to \mathrm{GL}(V)$ be a complex self-dual representation of G. Then, ρ is realisable over $\mathbb{R}$ if and only if V admits a non-degenerate G-invariant symmetric bilinear form.*

Proof. We will only prove one direction, namely the "only if" part. The other direction uses slightly more linear algebra than we have assumed so far. You can consult [3, Ch. II, Thm. 31] or [4, Theorem 73.3] for the "if" part.

Let ρ be realisable over $\mathbb{R}$. That means that if V is regarded as a real vector space (of twice its complex dimension), then there exists a subspace W that is

G-stable and such that $V = W \oplus iW$ as real vector spaces. The trick will be to construct a symmetric bilinear form on W and to extend it to V.

Let $(\_, \_)$ be any positive-definite symmetric bilinear form on W and define $\langle w_1, w_2\rangle = \frac{1}{|G|}\sum_{g\in G}(gw_1, gw_2)$. Clearly, $\langle \_, \_\rangle$ is G-invariant and still symmetric. It is also positive–definite (and in particular non-degenerate), since $\langle w, w\rangle = \frac{1}{|G|}\sum_{g\in G}(gw, gw) \geq 0$ with equality iff $gw = 0$ for all g, using positive-definiteness of $(\_, \_)$.

Now, write an arbitrary element v of V uniquely as $v = w_1 + iw_2$ and extend $\langle \_, \_\rangle$ to a $\mathbb{C}$-valued bilinear form on V by

$$\langle w_1 + iw_2, w_1' + iw_2'\rangle = \langle w_1, w_1'\rangle - \langle w_2, w_2'\rangle + i(\langle w_1, w_2'\rangle + \langle w_1', w_2\rangle).$$

It is immediate that this gives a non-degenerate symmetric G-invariant $\mathbb{C}$-bilinear form on V. □

Let us summarise again. There are three mutually exclusive possibilities for an irreducible complex representation ρ:

1. ρ is not self-dual. Equivalently, the character χ of ρ assumes at least one non-real value.

2. $\rho$is self-dual, so that χ is real, and moreover, ρ is realisable over $\mathbb{R}$.

3. ρ is self-dual, so that χ is real, but ρ itself is not realisable over $\mathbb{R}$.

Proposition 8.6. *An irreducible complex representation ρ is of type 1 if and only if it does not admit a non-degenerate G-invariant bilinear form. It is of type 2 if and only if it admits a symmetric non-degenerate G-invariant bilinear form. It is of type 3 if and only if it admits an alternating non-degenerate G-invariant bilinear form.*

Proof. We have already proven the first assertion. Now, let ρ be self-dual. Recall that G-invariant bilinear forms $\langle \_, \_\rangle$ are in bijection with homomorphisms $\rho \to \rho^*$. By Schur's lemma, such a form is therefore unique up to scalar multiples. Recall also from linear algebra, that we can write any bilinear form as the sum of a symmetric and an alternating one as follows:

$$\begin{aligned}\langle v, w\rangle_s &= \frac{1}{2}(\langle v, w\rangle + \langle w, v\rangle)\\ \langle v, w\rangle_a &= \frac{1}{2}(\langle v, w\rangle - \langle w, v\rangle)\\ \langle v, w\rangle &= \langle v, w\rangle_s + \langle v, w\rangle_a.\end{aligned}$$

Now, $\langle \_, \_\rangle_s$ and $\langle \_, \_\rangle_a$ are clearly also G-invariant, so exactly one of them is 0 by the uniqueness of $\langle \_, \_\rangle$. From the previous theorem, we know that $\langle \_, \_\rangle_a$ being zero corresponds to type 2, so the other case must correspond to type 3, and we are done. □

8.2 Tensor products, symmetric and alternating powers

Definition 8.7. Let V and W be vector spaces over a field K. The tensor product $V \otimes W$ is the vector space linearly spanned over K by symbols $v \otimes w$

for $v \in V$, $w \in W$, which satisfy the relations

$$\begin{aligned} k(v \otimes w) &= (kv) \otimes w = v \otimes (kw) \; \forall k \in K, v \in V, w \in W \\ (v + v') \otimes w &= (v \otimes w) + (v' \otimes w) \; \forall v, v' \in V, w \in W \\ v \otimes (w + w') &= (v \otimes w) + (v \otimes w') \; \forall v \in V, w, w' \in W. \end{aligned}$$

In other words, it is the quotient of the infinite-dimensional vector space with basis $\{v \otimes w : \; v \in V, w \in W\}$ modulo the subspace generated by $\{k(v \otimes w) - (kv) \otimes w, (kv) \otimes w - v \otimes (kw), (v+v') \otimes w - v \otimes w - v' \otimes w, v \otimes (w+w') - v \otimes w - v \otimes w'\}$.

If $v_1, \ldots, v_n$ is a basis of V and $w_1, \ldots, w_m$ is a basis of W, then $v_i \otimes w_j$: $1 \leq i \leq n$, $1 \leq j \leq m$ is easily seen to be a basis of $V \otimes W$. So, the dimension on $V \otimes W$ is $\dim V \cdot \dim W$. Note that a general element of $V \otimes W$ is of the form $\sum_k \tilde{v}_k \otimes \tilde{w}_k$ for $\tilde{v}_k \in V$, $\tilde{w}_k \in W$.

Proposition 8.8. *For any vector spaces U, V, W, we have $(U \otimes V) \otimes W \cong U \otimes (V \otimes W)$, $(U \oplus V) \otimes W \cong (U \otimes W) \oplus (V \otimes W)$. The isomorphisms are natural, in the sense that they do not depend on choices of bases.*

Proof. Check that the maps

$$\begin{aligned} (U \otimes V) \otimes W &\to U \otimes (V \otimes W) \\ (u \otimes v) \otimes w &\mapsto u \otimes (v \otimes w) \end{aligned}$$

and

$$\begin{aligned} (U \oplus V) \otimes W &\to (U \otimes W) \oplus (V \otimes W) \\ (u, v) \otimes w &\mapsto (u \otimes w, v \otimes w) \end{aligned}$$

are isomorphisms of vector spaces. □

Definition 8.9. Let $\rho : G \to \mathrm{GL}(V)$ and $\tau : G \to \mathrm{GL}(W)$ be representations of G over K. Then, $\rho \otimes \tau : G \to \mathrm{GL}(V \otimes W)$ is the G-representation defined by

$$\rho \otimes \tau(g)(v \otimes w) = \rho(g)v \otimes \tau(g)w.$$

The G-action respects the associativity and distributivity of Proposition 8.8, so that we get the same result for representations, not just for vector spaces.

Let g be represented by the matrix $A = (a_{i,j})$ with respect to a basis $v_1, \ldots, v_n$ of V and by the matrix $B = (b_{k,l})$ with respect to a basis $w_1, \ldots, w_m$. Let us work out the matrix of g on the basis

$$v_1 \otimes w_1, \ldots, v_1 \otimes w_m, v_2 \otimes w_1, \ldots, v_2 \otimes w_m, \ldots, v_n \otimes w_m.$$

We have

$$\begin{aligned} g(v_i \otimes w_k) &= gv_i \otimes gw_k \\ &= (a_{i,1}v_1 + \ldots + a_{i,n}v_n) \otimes (b_{k,1}w_1 + \ldots + b_{k,m}w_m) \end{aligned}$$

$$\sum_{j,l} a_{i,j} b_{k,l} v_j w_l.$$

From here, it immediately follows that the matrix of g with respect to the above basis on $V \otimes W$ is the $nm \times nm$ block matrix

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ a_{2,1}B & \cdots & b_{2,n}B \\ \vdots & \ddots & \vdots \\ a_{n,1}B & \cdots & a_{n,n}B \end{pmatrix}.$$

This calculation has some very useful consequences:

Corollary 8.10. *Let ρ, τ be complex representations of G with characters χ_ρ, χ_τ, respectively. Then, the character of $\rho \otimes \tau$ is $\chi_\rho \cdot \chi_\tau$.*

There is another way of seeing this: recall that the matrix corresponding to g under any representation is diagonalisable. Thus, the character of that representation is just the sum of eigenvalues of the g–action and there exists a basis of the corresponding vector space consisting of eigenvectors of g. Now, if $v \in V$ is an eigenvector of g with eigenvalue λ and $w \in W$ is an eigenvector with eigenvalue μ, then clearly $v \otimes w$ is an eigenvector of g with eigenvalue $\lambda\mu$.

Recall (from the proof of Theorem 3.3) that given two G–representations V,W over K, the vector space $\mathrm{Hom}_K(V, W)$ is a G-representation via $f^g(v) = gf(g^{-1}v)$. An extremely important consequence of our explicit calculation of matrices is

Corollary 8.11. *If V and W are two representations of G over a field K, then $V \otimes W \cong \mathrm{Hom}_K(V^*, W)$.*

Proof. We have already essentially computed the matrix of the action of G on $\mathrm{Hom}_K(V^*, W)$ in terms of the matrices of G on V and on W in the proof of Theorem 3.3. You should convince yourself that they are the same as the above matrices on the tensor product. □

Note that using associativity of tensor products, we can unambiguously define $V_1 \otimes \ldots \otimes V_n$ for any representations $V_1, \ldots, V_n$.

Definition 8.12. Let V be a G-representation. For any $n \in \mathbb{N}$, define the n-th tensor power of V by $V^{\otimes n} = \underbrace{V \otimes \ldots \otimes V}_{n\times}$.

Apart from the action of G on $V^{\otimes n}$, we also have an action of S_n by permuting the entries of each tensor: $\sigma(v_1 \otimes \ldots \otimes v_n) = v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}$. This action is immediately seen to commute with the action of G. In particular, if $V^{\otimes n} \cong \bigoplus_i W_i$ as a representation of S_n, where each $W_i \cong \rho_i^{\oplus k_i}$ with ρ_i denoting the distinct irreducible representations of S_n and with $k_i \in \mathbb{N}$, then each W_i is a G-subrepresentation of $V^{\otimes n}$.

Definition 8.13. Let K have characteristic 0 and let V be a G-representation of K. The n-th symmetric power of V, S^nV is defined as the G-subrepresentation of $V^{\otimes n}$ on which S_n acts trivially. The n-th alternating power Λ^nV is defined as the subspace on which S_n acts through the sign-character.

We can explicitly write down a basis for S^2V and for Λ^2V: let $v_1, \ldots, v_n$ be a basis of V. Then, it is immediate that

$$\begin{aligned} S^2V &= \langle v_i \otimes v_j + v_j \otimes v_i : 1 \leq i \leq j \leq n \rangle \\ \Lambda^2V &= \langle v_i \otimes v_j - v_j \otimes v_i : 1 \leq i < j \leq n \rangle. \end{aligned}$$

This immediately also gives us formulae for the dimensions of the symmetric square and the alternating square and for their characters:

$$\dim S^2V = \frac{n^2+n}{2}, \dim \Lambda^2V = \frac{n^2-n}{2},$$

and, denoting the eigenvalues of g on V by $\alpha_1, \ldots, \alpha_n$,

$$\begin{aligned} \chi_{S^2V}(g) &= \sum_{1 \leq i \leq j \leq n} \alpha_i \alpha_j \\ &= \frac{1}{2}\left((\sum_i \alpha_i)^2 + \sum_i \alpha_i^2 \right) = \frac{1}{2}\left(\chi_V(g)^2 + \chi_V(g^2) \right), \qquad (8.6) \\ \chi_{\Lambda^2V}(g) &= \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j \\ &= \frac{1}{2}\left((\sum_i \alpha_i)^2 - \sum_i \alpha_i^2 \right) = \frac{1}{2}\left(\chi_V(g)^2 - \chi_V(g^2) \right). \qquad (8.7) \end{aligned}$$

We have a decomposition of $V^{\otimes 2} = S^2V \oplus \Lambda^2V$ as G–representations. Suppose that V is an irreducible G–representation. Observe that Corollary 8.11 together with Schur's Lemma tells us that

$$\langle \chi_{V \otimes V}, \mathbf{1} \rangle = \begin{cases} 1, & V \cong V^* \\ 0, & \text{otherwise} \end{cases}.$$

In particular, if V is not self-dual, then both $\langle \chi_{S^2V}, \mathbf{1} \rangle_G$ and $\langle \chi_{\Lambda^2V}, \mathbf{1} \rangle_G$ are zero, while if V is self–dual, then exactly one of the inner products is 1 and the other one is 0. Which one of the two is non-trivial is a crucial characteristic of self-dual irreducible representations.

8.3 Realisability over $\mathbb{R}$

Definition 8.14. Let χ be a class function of a group G. The Frobenius–Schur indicator of χ is defined as

$$s_2(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

Proposition 8.15. *Let χ be an irreducible character of G. Then $s_2(\chi) \in \{-1, 0, 1\}$. Moreover,*

- *$s_2(\chi) = 0$ if and only if χ is not real valued;*
- *$s_2(\chi) = 1$ if and only if the representation of χ can be realised over $\mathbb{R}$, i.e. if the associated vector space carries a non-degenerate symmetric G–invariant bilinear pairing;*

- $s_2(\chi) = -1$ *if and only if* χ *is real-valued but the representation cannot be realised over* $\mathbb{R}$*, i.e. if the associated vector space carries a non-degenerate alternating* G*–invariant bilinear pairing.*

Proof. Using equation (8.6) and (8.7), we can write

$$\chi^2 = \frac{1}{2}(\chi_{S^2V}(g) - \chi_{\Lambda^2 V}(g)),$$

so that $s_2(\chi) = \langle \chi_{S^2V}, \mathbf{1}\rangle_G - \langle \chi_{\Lambda^2 V}, \mathbf{1}\rangle_G$. We have already observed that if χ is not self–dual, then both inner products are 0, and otherwise exactly one of them is 1. It follows that $s_2(\chi) \in \{-1, 0, 1\}$ with $s_2(\chi) = 0$ if and only if χ is not real valued. Assume for the rest of the proof that χ is real valued. We claim that $\langle \chi_{S^2V}, \mathbf{1}\langle_G = 1$ if and only if V admits a symmetric non-degenerate G–invariant bilinear pairing. Indeed, a bilinear pairing

$$\langle \_, \_\rangle : V \times V \longrightarrow \mathbb{C}$$

is the same as a linear map $\langle \_, \_\rangle : V \otimes V \longrightarrow \mathbb{C}$. In other words, the dual of the vector space $V \otimes V$ is the space of bilinear forms on V. Namely, given $f : V \otimes V \to \mathbb{C}$, define a bilinear form $\langle \_, \_\rangle_f$ on V by

$$\langle v, w\rangle_f = f(v \otimes w).$$

This form is G-invariant if and only if $f \in (V \otimes V)^G$. Now, the decomposition $V^{\otimes 2} = S^2V \oplus \Lambda^2 V$ induces the corresponding decomposition of dual spaces. Moreover, an element of $(S^2V)^*$ induces a symmetric bilinear form on V: given $f : (S^2V)^* \to \mathbb{C}$, define $\langle \_, \_\rangle_f$ by

$$\langle v, w\rangle_f = f(v \otimes w + w \otimes v),$$

and again this form in G-invariant if and only if f is fixed by the G-action on S^2V. Similarly, an element of $(\Lambda^2 V)^*$ gives an alternating bilinear form. So, we deduce that

$$\begin{aligned} (S^2V)^G &\neq 0 \quad \Leftrightarrow \text{ there exists a } G\text{-invariant symmetric bilinear form on } V, \\ (\Lambda^2 V)^G &\neq 0 \quad \Leftrightarrow \text{ there exists a } G\text{-invariant alternating bilinear form on} V, \end{aligned}$$

as claimed. □

We finish our discussion of realisability over $\mathbb{R}$ by considering the Wedderburn components of the real group algebra $\mathbb{R}G$. Recall that for general fields K of characteristic coprime to $|G|$, Wedderburn blocks of KG are of the form $M_n(D)$, where D are division algebras over K. The division algebras D are the endomorphism rings of the simple KG– modules. By a theorem of Burnside, the only division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$.

Theorem 8.16. *Let* ρ *be an irreducible complex representation of* G*.*

1. ρ *is not self-dual if and only if* $\rho \oplus \rho^*$ *is realisable over* $\mathbb{R}$ *and is a simple* $\mathbb{R}G$*–module with the corresponding Wedderburn block of* $\mathbb{R}G$ *equal to* $M_n(\mathbb{C})$*.*

2. ρ *is realisable over* $\mathbb{R}$ *(and therefore a simple* $\mathbb{R}G$*–module) if and only if the corresponding Wedderburn block of* $\mathbb{R}G$ *is* $M_n(\mathbb{R})$*.*

3. *ρ is self–dual but not realisable over $\mathbb{R}$ if and only if $\rho \oplus \rho$ is realisable over $\mathbb{R}$ and is a simple $\mathbb{R}G$–module with corresponding Wedderbun block $M_n(\mathbb{H})$. Such a representation is called* quaternionic *or* symplectic.

Sketch proof. The basic idea for proving that $\rho \oplus \rho^*$ (case 1) and $\rho \oplus \rho$ (case 3) are realisable over $\mathbb{R}$ is to construct a symmetric non–degenerate G–invariant bilinear pairing on each of them. For example, in case 3, let $[\_, \_]$ be a non–degenerate G–invariant alternating bilinear pairing on ρ. Define $\langle \_, \_ \rangle$ on $\rho \oplus \rho$ by

$$\langle (u_1, u_2), (v_1, v_2) \rangle = [u_1, v_1] \cdot [u_2, v_2].$$

Check that this is G-invariant, non–degenrate, bilinear, and symmetric. To define a symmetric pairing in case 1 is an exercise.

Next, notice that the three different real division algebras have different dimensions over $\mathbb{R}$, so it will suffice to determine the dimension of the endomorphism ring of the simple $\mathbb{R}G$–module in each case. Now, if τ is a $\mathbb{C}G$–module that is realisable over $\mathbb{R}$ and $\tau_{\mathbb{R}}$ is the corresponding $\mathbb{R}G$–module, then one can show (exercise) that

$$\dim_{\mathbb{R}} \operatorname{End}_{\mathbb{R}G}(\tau_{\mathbb{R}}) = \dim_{\mathbb{C}} \operatorname{End}_{\mathbb{C}G}(\tau),$$

the latter in turn being equal to $\langle \tau, \tau \rangle_G$. The result now follows from $\langle \rho, \rho \rangle_G = 1$, $\langle \rho \oplus \rho^*, \rho \oplus \rho^* \rangle_G = 2$ when ρ is not self–dual, and $\langle 2\rho, 2\rho \rangle_G = 4$. □

Example 8.17. Let us closely inspect the example of $G = \mathrm{SL}_2(\mathbb{F}_3) \cong Q_8 \rtimes C_3$. First, recall the character table of G. We label the columns by the sizes of the conjugacy classes and by the orders of their elements:

size	1	1	4	4	6	4	4
order	1	2	3	3	4	6	6
$\mathbf{1} = \chi_1$	1	1	1	1	1	1	1
χ_2	1	1	$\overline{\omega}$	ω	1	ω	$\overline{\omega}$
χ_3	1	1	ω	$\overline{\omega}$	1	$\overline{\omega}$	ω
τ_4	2	-2	-1	-1	0	1	1
τ_5	2	-2	$-\overline{\omega}$	$-\omega$	0	ω	$\overline{\omega}$
τ_6	2	-2	$-\omega$	$-\overline{\omega}$	0	$\overline{\omega}$	ω
τ_7	3	3	0	0	-1	0	0

Here, ω is a primitive cube root of unity. We see immediately that the characters χ_2, χ_3, τ_5, and τ_6 are not self–dual, while the other three are. To work out which ones are realisable over $\mathbb{Q}$, we can compute the Frobenius-Schur indicators. But for that, we need to know which conjugacy classes square to which. Clearly, an element of order 2 squares to the identity, while an element of order 4 squares to an element of order 2. The square of an element of order 3 or 6 has order 3, and there is therefore an ambiguity. In this particular case, we don't need to know whether the two conjugacy classes of elements of order 3 square to each other (i.e. are inverses of each other) or not, since the characters τ_4 and τ_7 take the same value on both order 3 conjugacy classes. But also note, that here we can actually resolve the ambiguity: the number of self–inverse conjugacy classes is equal to the number of real characters (exercise sheet), so that neither the order 3 conjugacy classes nor the order 6 conjugacy classes can be self–inverse.

So, we can now compute

$$\begin{aligned} s_2(\tau_4) &= \frac{1}{24}(2+2+4\cdot(-1)+4\cdot(-1)+6\cdot(-2)+4\cdot(-1)+4\cdot(-1)) = -1, \\ s_2(\tau_7) &= \frac{1}{24}(3+3+6\cdot 3) = 1. \end{aligned}$$

We deduce that τ_7 is realisable over $\mathbb{R}$, but τ_4 is not, only $2\tau_4$ is. It is worth noting that since τ_4 is two–dimensional, it appears twice in the regular representation. So, using the idempotent of $\mathbb{C}G$ corresponding to τ_4, we could get an explicit realisation of $2\tau_4$ as a subrepresentation of $\mathbb{C}G$ or of $\mathbb{R}G$.

8.4 Counting roots in groups

The last topic on Frobenius-Schur indicators will be a group theoretic application of the machinery we have developed in this section.

Definition 8.18. Let G be a finite group. Define the square root counting function r_2 by

$$\begin{aligned} r_2 : G &\to \mathbb{N} \\ g &\mapsto \#\{h \in G :\ h^g = g\}. \end{aligned}$$

For example $r_2(1) - 1$ is the number of elements of order 2 in G.

Lemma 8.19. *The function r_2 is a class function.*

Proof. If $g' = xgx^{-1}$, then $h \mapsto xhx^{-1}$ is a bijection between square roots of g and square roots of g', so $r_2(g) = r_2(g')$. □

We can thus write $r_2 = \sum_{\chi \in \mathrm{Irr}(G)} \alpha_\chi \chi$ for some scalars α_χ. Let us compute these coefficients:

$$\begin{aligned} \langle r_2, \chi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} r_2(g)\chi(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{h \in G} \delta_{h^2,g}\chi(h^2) \\ &= \frac{1}{|G|} \sum_{h \in G} \sum_{g \in G} \delta_{h^2,g}\chi(h^2) \\ &= \frac{1}{|G|} \sum_{h \in G} \chi(h^2) = s_2(\chi). \end{aligned}$$

We deduce:

Proposition 8.20. *The number of square roots of a group element is given by*

$$r_2(g) = \sum_{\chi \in \mathrm{Irr}(G)} s_2(\chi)\chi(g).$$

Corollary 8.21. *Suppose that G has no symplectic representations. Then r_2 assumes its maximum at the identity element.*

Proof. This follows immediately from the two facts $s_2(\chi) \in \{0, 1\}$ and $\chi(1) \geq |\chi(g)|$ for all $g \in G$. □

References

[1] R. B. Ash, Abstract Algebra, Dover Books of Mathematics, available online.

[2] I. M. Isaacs, Character Theory of Finite Groups, Academic Press, 1978.

[3] J.-P. Serre, Linear Representations of Finite Groups, Springer, Graduate Textxs in Mathematics 42, 1977.

[4] C. W. Curtis and I. Reiner, Methods of Representation Theory, Vol. II, John Wiley & Sons, 1987.