VI

Representation Theory

Part VI: Contents

19 Representations of algebras **233**

19.1 Algebras . . . 233
19.2 Representations . . . 234
19.3 Direct sums . . . 236
19.4 Irreducible and indecomposable representations . . . 238
19.5 Morphisms of representations . . . 239
19.6 The representations of $\mathrm{Mat}_d(k)$ . . . 241
19.7 A few harder problems to think about . . . 242

20 Semisimple algebras **245**

20.1 Schur's lemma continued . . . 245
20.2 Density theorem . . . 247
20.3 Semisimple algebras . . . 249
20.4 Maschke's theorem . . . 250
20.5 Example: the representations of $\mathbb{C}[S_3]$ . . . 251
20.6 A few harder problems to think about . . . 252

21 Characters **253**

21.1 Definitions . . . 253
21.2 The dual space modulo the commutator . . . 254
21.3 Orthogonality of characters . . . 255
21.4 Examples of character tables . . . 257
21.5 A few harder problems to think about . . . 259

22 Some applications **261**

22.1 Frobenius divisibility . . . 261
22.2 Burnside's theorem . . . 262
22.3 Frobenius determinant . . . 263

19 Representations of algebras

In the 19th century, the word "group" hadn't been invented yet; all work was done with subsets of $\mathrm{GL}(n)$ or S_n. Only much later was the abstract definition of a group was given, an abstract set G which was an object in its own right.

While this abstraction is good for some reasons, it is often also useful to work with concrete representations. This is the subject of representation theory. Linear algebra is easier than abstract algebra, so if we can take a group G and represent it concretely as a set of matrices in $\mathrm{GL}(n)$, this makes them easier to study. This is the *representation theory of groups*: how can we take a group and represent its elements as matrices?

§19.1 Algebras

Prototypical example for this section: $k[x_1, \dots, x_n]$ *and* $k[G]$.

Rather than working directly with groups from the beginning, it will be more convenient to deal with so-called k-algebras. This setting is more natural and general than that of groups, so once we develop the theory of algebras well enough, it will be fairly painless to specialize to the case of groups.

Colloquially,

An associative k-algebra is a possibly noncommutative ring with a copy of k inside it. It is thus a k-vector space.

I'll present examples before the definition:

Example 19.1.1 (Examples of k-algebras)
Let k be any field. The following are examples of k-algebras:

(a) The field k itself.

(b) The polynomial ring $k[x_1, \dots, x_n]$.

(c) The set of $n \times n$ matrices with entries in k, which we denote by $\mathrm{Mat}_n(k)$. Note the multiplication here is not commutative.

(d) The set $\mathrm{Mat}(V)$ of linear maps $T \colon V \to V$, with multiplication given by the composition of operators. (Here V is some vector space over k.) This is really the same as the previous example.

Definition 19.1.2. Let k be a field. A **k-algebra** A is a *possibly noncommutative* ring, equipped with a ring homomorphism $k \hookrightarrow A$, whose image is the "copy of k". (In particular, $1_k \mapsto 1_A$.)

Thus we can consider k as a subset of A, and we then additionally require $\lambda \cdot a = a \cdot \lambda$ for each $\lambda \in k$ and $a \in A$.

If the multiplication operation is also commutative, then we say A is a **commutative algebra**.

Definition 19.1.3. Equivalently, a **k-algebra** A is a k-*vector space* which also has an associative, bilinear multiplication operation (with an identity 1_A). The "copy of k" is obtained by considering elements $\lambda 1_A$ for each $\lambda \in k$ (i.e. scaling the identity by the elements of k, taking advantage of the vector space structure).

Abuse of Notation 19.1.4. Some other authors don't require A to be associative or to have an identity, so to them what we have just defined is an "associative algebra with 1". However, this is needlessly wordy for our purposes.

Example 19.1.5 (Group algebra)

The **group algebra** $k[G]$ is the k-vector space whose *basis elements* are the elements of a group G, and where the product of two basis elements is the group multiplication. For example, suppose $G = \mathbb{Z}/2\mathbb{Z} = \{1_G, x\}$. Then

$$k[G] = \{a1_G + bx \mid a, b \in k\}$$

with multiplication given by

$$(a1_G + bx)(c1_G + dx) = (ac + bd)1_G + (bc + ad)x.$$

Question 19.1.6. When is $k[G]$ commutative?

The example $k[G]$ is very important, because (as we will soon see) a representation of the algebra $k[G]$ amounts to a representation of the group G itself.

It is worth mentioning at this point that:

Definition 19.1.7. A **homomorphism** of k-algebras A, B is a linear map $T\colon A \to B$ which respects multiplication (i.e. $T(xy) = T(x)T(y)$) and which sends 1_A to 1_B. In other words, T is both a homomorphism as a ring and as a vector space.

We will also need to recall the "product ring" from Example 4.3.8, but for algebras, we will prefer a different name and notation.

Definition 19.1.8. Given k-algebras A and B, the **direct sum** $A \oplus B$ is defined as pairs $a + b$, where addition is done in the obvious way, but we declare $ab = 0$ for any $a \in A$ and $b \in B$.

Question 19.1.9. Show that $1_A + 1_B$ is the multiplicative identity of $A \oplus B$.

Equivalently, similar to Definition 9.3.1 and Example 4.3.8, you can define the direct sum $A \oplus B$ to be the set of pairs (a, b), where multiplication is defined by $(a, b)(a', b') = (aa', bb')$. In this notation, $(1_A, 1_B)$ would be the multiplicative identity of $A \oplus B$.

§19.2 Representations

Prototypical example for this section: $k[S_3]$ *acting on* $k^{\oplus 3}$ *is my favorite.*

Definition 19.2.1. A **representation** of a k-algebra A (also a **left A-module**) is:

(i) A k-vector space V, and

(ii) An *action* $\cdot$ of A on V: thus, for every $a \in A$ we can take $v \in V$ and act on it to get $a \cdot v$. This satisfies the usual axioms:

- $(a + b) \cdot v = a \cdot v + b \cdot v$, $a \cdot (v + w) = a \cdot v + a \cdot w$, and $(ab) \cdot v = a \cdot (b \cdot v)$.
- $\lambda \cdot v = \lambda v$ for $\lambda \in k$. In particular, $1_A \cdot v = v$.

Definition 19.2.2. The action of A can be more succinctly described as saying that there is a *k-algebra homomorphism* $\rho \colon A \to \mathrm{Mat}(V)$. (So $a \cdot v = \rho(a)(v)$.) Thus we can also define a **representation** of A as a pair

$$(V, \rho \colon A \to \mathrm{Mat}(V)) .$$

This is completely analogous to how a group action G on a set X with n elements just amounts to a group homomorphism $G \to S_n$. From this perspective, what we are really trying to do is:

If A is an algebra, we are trying to *represent* the elements of A as matrices.

Abuse of Notation 19.2.3. While a representation is a pair (V, ρ) of *both* the vector space V and the action ρ, we frequently will just abbreviate it to "V". This is probably one of the worst abuses I will commit, but everyone else does it and I fear the mob.

Abuse of Notation 19.2.4. Rather than $\rho(a)(v)$ we will just write $\rho(a)v$.

Example 19.2.5 (Representations of $\mathrm{Mat}(V)$)

(a) Let $A = \mathrm{Mat}_2(\mathbb{R})$. Then there is a representation $(\mathbb{R}^{\oplus 2}, \rho)$ where a matrix $a \in A$ just acts by $a \cdot v = \rho(a)(v) = a(v)$.

(b) More generally, given a vector space V over any field k, there is an obvious representation of $A = \mathrm{Mat}(V)$ by $a \cdot v = \rho(a)(v) = a(v)$ (since $a \in \mathrm{Mat}(V)$).

From the matrix perspective: if $A = \mathrm{Mat}(V)$, then we can just represent A as matrices over V.

(c) There are other representations of $A = \mathrm{Mat}_2(\mathbb{R})$. A silly example is the representation $(\mathbb{R}^{\oplus 4}, \rho)$ given by

$$\rho : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix} .$$

More abstractly, viewing $\mathbb{R}^{\oplus 4}$ as $(\mathbb{R}^{\oplus 2}) \oplus (\mathbb{R}^{\oplus 2})$, this is $a \cdot (v_1, v_2) = (a \cdot v_1, a \cdot v_2)$.

Example 19.2.6 (Representations of polynomial algebras)

(a) Let $A = k$. Then a representation of k is just any k-vector space V.

(b) If $A = k[x]$, then a representation (V, ρ) of A amounts to a vector space V plus the choice of a linear map $T \in \mathrm{Mat}(V)$ (by $T = \rho(x)$).

(c) If $A = k[x]/(x^2)$ then a representation (V, ρ) of A amounts to a vector space V plus the choice of a linear map $T \in \mathrm{Mat}(V)$ satisfying $T^2 = 0$.

(d) We can create arbitrary "functional equations" with this pattern. For example, if $A = k[x,y]/(x^2 - x + y, y^4)$ then representing A by V amounts to finding commuting operators $S, T \in \operatorname{Mat}(V)$ satisfying $S^2 = S - T$ and $T^4 = 0$.

Example 19.2.7 (Representations of groups)

(a) Let $A = \mathbb{R}[S_3]$. Then let

$$V = \mathbb{R}^{\oplus 3} = \{(x,y,z) \mid x,y,z \in \mathbb{R}\}.$$

We can let A act on V as follows: given a permutation $\pi \in S_3$, we permute the corresponding coordinates in V. So for example, if

$$\text{If } \pi = (1\ 2) \text{ then } \pi \cdot (x,y,z) = (y,x,z).$$

This extends linearly to let A act on V, by permuting the coordinates.

From the matrix perspective, what we are doing is representing the permutations in S_3 as permutation matrices on $k^{\oplus 3}$, like

$$(1\ 2) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

(b) More generally, let $A = k[G]$. Then a representation (V, ρ) of A amounts to a group homomorphism $\psi \colon G \to \operatorname{GL}(V)$. (In particular, $\rho(1_G) = \operatorname{id}_V$.) We call this a **group representation** of G.

Example 19.2.8 (Regular representation)

Any k-algebra A is a representation (A, ρ) over itself, with $a \cdot b = \rho(a)(b) = ab$ (i.e. multiplication given by A). This is called the **regular representation**, denoted $\operatorname{Reg}(A)$.

§19.3 Direct sums

Prototypical example for this section: The example with $\mathbb{R}[S_3]$ seems best.

Definition 19.3.1. Let A be k-algebra and let $V = (V, \rho_V)$ and $W = (W, \rho_W)$ be two representations of A. Then $V \oplus W$ is a representation, with action ρ given by

$$a \cdot (v, w) = (a \cdot v, a \cdot w).$$

This representation is called the **direct sum** of V and W.

Example 19.3.2

Earlier we let $\text{Mat}_2(\mathbb{R})$ act on $\mathbb{R}^{\oplus 4}$ by

$$\rho : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}.$$

So this is just a direct sum of two two-dimensional representations.

You can also view the vectors of $\mathbb{R}^{\oplus 4}$ as two vectors in $\mathbb{R}^{\oplus 2}$ "stacked horizontally" as $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$, so the action would be given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

Remark 19.3.3 — Perhaps this is the reason why people tend to write V as the representation without the accompanied ρ_V, as long as it's possible to embed the k-algebra A into a subalgebra of $\text{Mat}_d(k)$, then V can be isomorphically embedded as a subrepresentation of $(k^{\oplus d})^{\oplus m}$, being m copies of the obvious $k^{\oplus d}$ representation stacked horizontally.

More generally, given representations (V, ρ_V) and (W, ρ_W) the representation ρ of $V \oplus W$ looks like

$$\rho(a) = \begin{bmatrix} \rho_V(a) & 0 \\ 0 & \rho_W(a) \end{bmatrix}.$$

Example 19.3.4 (Representation of S_n decomposes)

Let $A = \mathbb{R}[S_3]$ again, acting via permutation of coordinates on

$$V = \mathbb{R}^{\oplus 3} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

Consider the two subspaces

$$\begin{aligned} W_1 &= \{(t, t, t) \mid t \in \mathbb{R}\} \\ W_2 &= \{(x, y, z) \mid x + y + z = 0\}. \end{aligned}$$

Note $V = W_1 \oplus W_2$ as vector spaces. But each of W_1 and W_2 is a subrepresentation (since the action of A keeps each W_i in place), so $V = W_1 \oplus W_2$ as representations too.

Direct sums also come up when we play with algebras.

Proposition 19.3.5 (Representations of $A \oplus B$ are $V_A \oplus V_B$)

Let A and B be k-algebras. Then every representation of $A \oplus B$ is of the form

$$V_A \oplus V_B$$

where V_A and V_B are representations of A and B, respectively.

Example 19.3.6

Take $A = B = \text{Mat}_2(\mathbb{R})$. There are two obvious representations of the k-algebra $A \oplus B$, V_A and V_B, corresponds to the action of A and B respectively.

Each of V_A and V_B are isomorphic to $\mathbb{R}^{\oplus 2}$ as $\mathbb{R}$-vector spaces.

What this proposition says is that, you cannot "mix" the action of A and B in order to get some representation $V \cong \mathbb{R}^2$ of $A \oplus B$, such as by $(a+b) \cdot v = a \cdot v + 2b \cdot v$ for $a \in A$ and $b \in B$.

Sketch of Proof. Let (V, ρ) be a representation of $A \oplus B$. For any $v \in V$, $\rho(1_A + 1_B)v = \rho(1_A)v + \rho(1_B)v$. One can then set $V_A = \{\rho(1_A)v \mid v \in V\}$ and $V_B = \{\rho(1_B)v \mid v \in V\}$. These are disjoint, since if $\rho(1_A)v = \rho(1_B)v'$, we have $\rho(1_A)v = \rho(1_A 1_A)v = \rho(1_A 1_B)v' = 0_V$, and similarly for the other side. $\square$

In the example above, if you see the representation $V_A \oplus V_B$ as $\mathbb{R}^4$, then any element in A acting on an element in $V_A \oplus V_B$ would zero out the V_B-component of the vector.

So, the key idea of the proof is:

The A and B component of $A \oplus B$ is used to act on V, in order to project the vector space V into the components V_A and V_B to separate out the subrepresentations.

§19.4 Irreducible and indecomposable representations

Prototypical example for this section: $k[S_3]$ decomposes as the sum of two spaces.

One of the goals of representation theory will be to classify all possible representations of an algebra A. If we want to have a hope of doing this, then we want to discard "silly" representations such as

$$\rho : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}$$

and focus our attention instead on "irreducible" representations. This motivates:

Definition 19.4.1. Let V be a representation of A. A **subrepresentation** $W \subseteq V$ is a subspace W with the property that for any $a \in A$ and $w \in W$, $a \cdot w \in W$. In other words, this subspace is invariant under actions by A.

Thus for example if $V = W_1 \oplus W_2$ for representations W_1, W_2 then W_1 and W_2 are subrepresentations of V.

Definition 19.4.2. If V has no proper nonzero subrepresentations then it is **irreducible**. If there is no pair of proper subrepresentations W_1, W_2 such that $V = W_1 \oplus W_2$, then we say V is **indecomposable**.

Definition 19.4.3. For brevity, an **irrep** of an algebra/group is a *finite-dimensional* irreducible representation.

Example 19.4.4 (Representation of S_n decomposes)
Let $A = \mathbb{R}[S_3]$ again, acting via permutation of coordinates on

$$V = \mathbb{R}^{\oplus 3} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

Consider again the two subspaces

$$\begin{aligned} W_1 &= \{(t, t, t) \mid t \in \mathbb{R}\} \\ W_2 &= \{(x, y, z) \mid x + y + z = 0\}. \end{aligned}$$

As we've seen, $V = W_1 \oplus W_2$, and thus V is not irreducible. But one can show that W_1 and W_2 are irreducible (and hence indecomposable) as follows.

- For W_1 it's obvious, since W_1 is one-dimensional.
- For W_2, consider any vector $w = (a, b, c)$ with $a + b + c = 0$ and not all zero. Then WLOG we can assume $a \neq b$ (since not all three coordinates are equal). In that case, $(1\ 2)$ sends w to $w' = (b, a, c)$. Then w and w' span W_2.

Thus V breaks down completely into irreps.

Unfortunately, if W is a subrepresentation of V, then it is not necessarily the case that we can find a supplementary vector space W' such that $V = W \oplus W'$. Put another way, if V is reducible, we know that it has a subrepresentation, but a decomposition requires *two* subrepresentations. Here is a standard counterexample:

Exercise 19.4.5. Let $A = \mathbb{R}[x]$, and $V = \mathbb{R}^{\oplus 2}$ be the representation with action

$$\rho(x) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Show that the only subrepresentation is $W = \{(t, 0) \mid t \in \mathbb{R}\}$. So V is not irreducible, but it is indecomposable.

Here is a slightly more optimistic example, and the "prototypical example" that you should keep in mind.

Exercise 19.4.6. Let $A = \operatorname{Mat}_d(k)$ and consider the obvious representation $k^{\oplus d}$ of A that we described earlier. Show that it is irreducible. (This is obvious if you understand the definitions well enough.)

§19.5 Morphisms of representations

We now proceed to define the morphisms between representations.

Definition 19.5.1. Let (V, ρ_V) and (W, ρ_W) be representations of A. An **intertwining operator**, or **morphism**, is a linear map $T \colon V \to W$ such that

$$T(a \cdot v) = a \cdot T(v)$$

for any $a \in A$, $v \in V$. (Note that the first $\cdot$ is the action of ρ_V and the second $\cdot$ is the action of ρ_W.) This is exactly what you expect if you think that V and W are "left A-modules". If T is invertible, then it is an **isomorphism** of representations and we say $V \cong W$.

Remark 19.5.2 (For commutative diagram lovers) — The condition $T(a \cdot v) = a \cdot T(v)$ can be read as saying that

$$\begin{tikzcd} V \arrow[r, "\rho_1(a)"] \arrow[d, "T"'] & V \arrow[d, "T"] \\ W \arrow[r, "\rho_2(a)"'] & W \end{tikzcd}$$

commutes for any $a \in A$.

Remark 19.5.3 (For category lovers) — A representation is just a "bilinear" functor from an abelian one-object category $\{*\}$ (so $\operatorname{Hom}(*,*) \cong A$) to the abelian category Vect_k. Then an intertwining operator is just a *natural transformation*.

Here are some examples of intertwining operators.

Example 19.5.4 (Intertwining operators)

(a) For any $\lambda \in k$, the scalar map $T(v) = \lambda v$ is intertwining.

(b) If $W \subseteq V$ is a subrepresentation, then the inclusion $W \hookrightarrow V$ is an intertwining operator.

(c) The projection map $V_1 \oplus V_2 \twoheadrightarrow V_1$ is an intertwining operator.

(d) Let $V = \mathbb{R}^{\oplus 2}$ and represent $A = k[x]$ by (V, ρ) where

$$\rho(x) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Thus $\rho(x)$ is rotation by $90°$ around the origin. Let T be rotation by $30°$. Then $T : V \to V$ is intertwining (the rotations commute).

Example 19.5.5 (A non-example: Representation of $\operatorname{Mat}(V)$)

Let $A = \operatorname{Mat}_2(\mathbb{R}) \oplus \operatorname{Mat}_2(\mathbb{R})$. Then A can be viewed as a subset of $\operatorname{Mat}_4(\mathbb{R})$ of the matrices of the form

$$\begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & e & f \\ 0 & 0 & g & h \end{bmatrix}.$$

There are two obvious irreps of A, given by V_1 consisting of the vectors in $\mathbb{R}^4$ of the form $(m, n, 0, 0)$, and V_2 consisting of the vectors in $\mathbb{R}^4$ of the form $(0, 0, p, q)$.

In this case, even though V_1 and V_2 are isomorphic as $\mathbb{R}$-vector spaces, they're not isomorphic as representations of A – so any intertwining operator from V_1 to V_2 must be identically zero.

Exercise 19.5.6 (Kernel and image are subrepresentations)**.** Let $T \colon V \to W$ be an intertwining operator.

(a) Show that $\ker T \subseteq V$ is a subrepresentation of V.

(b) Show that $\operatorname{im} T \subseteq W$ is a subrepresentation of W.

The previous exercise gives us the famous Schur's lemma.

Theorem 19.5.7 (Schur's lemma)

Let V and W be representations of a k-algebra A. Let $T \colon V \to W$ be a *nonzero* intertwining operator. Then

(a) If V is irreducible, then T is injective.

(b) If W is irreducible, then T is surjective.

In particular if both V and W are irreducible then T is an isomorphism.

An important special case is if k is algebraically closed: then the only intertwining operators $T \colon V \to V$ are multiplication by a constant.

Theorem 19.5.8 (Schur's lemma for algebraically closed fields)

Let k be an algebraically closed field. Let V be an irrep of a k-algebra A. Then any intertwining operator $T \colon V \to V$ is multiplication by a scalar.

Exercise 19.5.9. Use the fact that T has an eigenvalue λ to deduce this from Schur's lemma. (Consider $T - \lambda \cdot \mathrm{id}_V$, and use Schur to deduce it's zero.)

We have already seen the counterexample of rotation by 90° for $k = \mathbb{R}$; this was the same counterexample we gave to the assertion that all linear maps have eigenvalues.

§19.6 The representations of $\mathrm{Mat}_d(k)$

To give an example of the kind of progress already possible, we prove:

Theorem 19.6.1 (Representations of $\mathrm{Mat}_d(k)$)

Let k be any field, d be a positive integer and let $W = k^{\oplus d}$ be the obvious representation of $A = \mathrm{Mat}_d(k)$. Then the only finite-dimensional representations of $\mathrm{Mat}_d(k)$ are $W^{\oplus n}$ for some positive integer n (up to isomorphism). In particular, it is irreducible if and only if $n = 1$.

For concreteness, I'll just sketch the case $d = 2$, since the same proof applies verbatim to other situations. This shows that the examples of representations of $\mathrm{Mat}_2(\mathbb{R})$ we gave earlier are the only ones.

As we've said this is essentially a functional equation. The algebra $A = \mathrm{Mat}_2(k)$ has basis given by four matrices

$$E_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad E_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \qquad E_3 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad E_4 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

satisfying relations like $E_1 + E_2 = \mathrm{id}_A$, $E_i^2 = E_i$, $E_1E_2 = 0$, etc. So let V be a representation of A, and let $M_i = \rho(E_i)$ for each i; we want to classify the possible matrices M_i on V satisfying the same functional equations. This is because, for example,

$$\mathrm{id}_V = \rho(\mathrm{id}_A) = \rho(E_1 + E_2) = M_1 + M_2.$$

By the same token $M_1M_3 = M_3$. Proceeding in a similar way, we can obtain the following multiplication table:

$$\begin{array}{c|cccc} \times & M_1 & M_2 & M_3 & M_4 \\ \hline M_1 & M_1 & 0 & M_3 & 0 \\ M_2 & 0 & M_2 & 0 & M_4 \\ M_3 & 0 & M_3 & 0 & M_1 \\ M_4 & M_4 & 0 & M_2 & 0 \end{array} \qquad \text{and} \qquad M_1 + M_2 = \mathrm{id}_V$$

Note that each M_i is a linear map $V \to V$; for all we know, it could have hundreds of entries. Nonetheless, given the multiplication table of the basis E_i we get the corresponding table for the M_i.

So, in short, the problem is as follows:

Find all vector spaces V and quadruples of matrices M_i satisfying the multiplication table above.

Let $W_1 = M_1^{\mathrm{img}}(V)$ and $W_2 = M_2^{\mathrm{img}}(V)$ be the images of M_1 and M_2.

Claim 19.6.2. $V = W_1 \oplus W_2$.

Proof. First, note that for any $v \in V$ we have

$$v = \rho(\mathrm{id})(v) = (M_1 + M_2)v = M_1v + M_2v.$$

Moreover, we have that $W_1 \cap W_2 = \{0\}$, because if $M_1v_1 = M_2v_2$ then $M_1v_1 = M_1(M_1v_1) = M_1(M_2v_2) = 0$. □

Claim 19.6.3. $W_1 \cong W_2$.

Proof. Check that the maps

$$W_1 \xrightarrow{\times M_4} W_2 \quad \text{and} \quad W_2 \xrightarrow{\times M_3} W_1$$

are well-defined and mutually inverse. □

Now, let $e_1, \dots, e_n$ be basis elements of W_1; thus $M_4e_1, \dots, M_4e_n$ are basis elements of W_2. However, each $\{e_j, M_4e_j\}$ forms a basis of a subrepresentation isomorphic to $W = k^{\oplus 2}$ (what's the isomorphism?).

This finally implies that all representations of A are of the form $W^{\oplus n}$. In particular, W is irreducible because there are no representations of smaller dimension at all!

§19.7 A few harder problems to think about

Problem 19A†. Suppose we have *one-dimensional* representations $V_1 = (V_1, \rho_1)$ and $V_2 = (V_2, \rho_2)$ of A. Show that $V_1 \cong V_2$ if and only if $\rho_1(a)$ and $\rho_2(a)$ are multiplication by the same constant for every $a \in A$.

Problem 19B† (Schur's lemma for commutative algebras)**.** Let A be a *commutative* algebra over an algebraically closed field k. Prove that any irrep of A is one-dimensional.

Problem 19C***.** Let (V, ρ) be a representation of A. Then $\operatorname{Mat}(V)$ is a representation of A with action given by

$$a \cdot T = \rho(a) \circ T$$

for $T \in \operatorname{Mat}(V)$.

(a) Show that $\rho\colon \operatorname{Reg}(A) \to \operatorname{Mat}(V)$ is an intertwining operator.

(b) If V is d-dimensional, show that $\operatorname{Mat}(V) \cong V^{\oplus d}$ as representations of A.

Problem 19D***.** Fix an algebra A. Find all intertwining operators

$$T\colon \operatorname{Reg}(A) \to \operatorname{Reg}(A).$$

Problem 19E. Let (V, ρ) be an *indecomposable* (not irreducible) representation of an algebra A. Prove that any intertwining operator $T\colon V \to V$ is either nilpotent or an isomorphism.

(Note that Theorem 19.5.8 doesn't apply, since the field k may not be algebraically closed.)

20 Semisimple algebras

In what follows, **assume the field k is algebraically closed**.

Fix an algebra A and suppose you want to study its representations. We have a "direct sum" operation already. So, much like we pay special attention to prime numbers, we're motivated to study irreducible representations and then build all the representations of A from there.

Unfortunately, we have seen (Exercise 19.4.5) that there exists a representation which is not irreducible, and yet cannot be broken down as a direct sum (indecomposable). This is *weird and bad*, so we want to give a name to representations which are more well-behaved. We say that a representation is **completely reducible** if it doesn't exhibit this bad behavior.

Even better, we say a finite-dimensional algebra A is **semisimple** if all its finite-dimensional representations are completely reducible. So when we study finite-dimensional representations of semisimple algebras A, we just have to figure out what the irreps are, and then piecing them together will give all the representations of A.

In fact, semisimple algebras A have even nicer properties. The culminating point of the chapter is when we prove that A is semisimple if and only if $A \cong \bigoplus_i \operatorname{Mat}(V_i)$, where the V_i are the irreps of A (yes, there are only finitely many!).

In the end, we will see that the group algebras $k[G]$ of a finite group G are all semisimple (at least when k has characteristic 0), thus we're justified in focusing on studying the semisimple algebras.

Remark 20.0.1 (Digression) — The converse does not hold, however — if k has characteristic 0, not every finite-dimensional semisimple k-algebra is isomorphic to some group algebra. Classifying exactly when a k-algebra is isomorphic to a group algebra turns out to be a hard question, see `https://mathoverflow.net/q/314502`.

§20.1 Schur's lemma continued

Prototypical example for this section: For V irreducible, $\operatorname{Hom}_{\text{rep}}(V^{\oplus 2}, V^{\oplus 2}) \cong k^{\oplus 4}$.

Definition 20.1.1. For an algebra A and representations V and W, we let $\operatorname{Hom}_{\text{rep}}(V, W)$ be the set of intertwining operators between them. (It is also a k-algebra.)

By Schur's lemma (since k is algebraically closed, which again, we are taking as a standing assumption), we already know that if V and W are irreps, then

$$\operatorname{Hom}_{\text{rep}}(V, W) \cong \begin{cases} k & \text{if } V \cong W \\ 0 & \text{if } V \not\cong W. \end{cases}$$

Can we say anything more? For example, it also tells us that

$$\operatorname{Hom}_{\text{rep}}(V, V^{\oplus 2}) = k^{\oplus 2}.$$

The possible maps are $v \mapsto (c_1 v_1, c_2 v_2)$ for some choice of $c_1, c_2 \in k$.

More generally, suppose V is an irrep and consider $\operatorname{Hom}_{\text{rep}}(V^{\oplus m}, V^{\oplus n})$. Intertwining operators $T\colon V^{\oplus m} \to V^{\oplus n}$ are determined completely by the mn choices of compositions

$$V \hookrightarrow V^{\oplus m} \xrightarrow{T} V^{\oplus n} \twoheadrightarrow V$$

where the first arrow is inclusion to the ith component of $V^{\oplus m}$ (for $1 \le i \le m$) and the second arrow is inclusion to the jth component of $V^{\oplus n}$ (for $1 \le j \le n$). However, by Schur's lemma on each of these compositions, we know they must be constant.

Thus, $\operatorname{Hom}_{\text{rep}}(V^{\oplus n}, V^{\oplus m})$ consist of $n \times m$ "matrices" of constants, and the map is provided by

$$\begin{bmatrix} c_{11} & c_{12} & \dots & c_{1(n-1)} & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2(n-1)} & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{m(n-1)} & c_{mn} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in V^{\oplus m}$$

where the $c_{ij} \in k$ but $v_i \in V$; note the type mismatch! This is *not* just a k-linear map $V^{\oplus n} \to V^{\oplus m}$; rather, the outputs are m *linear combinations* of the inputs.

More generally, we have:

Theorem 20.1.2 (Schur's lemma for completely reducible representations)

Let V and W be completely reducible representations, and set $V = \bigoplus V_i^{\oplus n_i}$, $W = \bigoplus V_i^{\oplus m_i}$ for integers $n_i, m_i \ge 0$, where each V_i is an irrep. Then

$$\operatorname{Hom}_{\text{rep}}(V, W) \cong \bigoplus_i \operatorname{Mat}_{m_i \times n_i}(k)$$

meaning that an intertwining operator $T \colon V \to W$ amounts to, for each i, an $m_i \times n_i$ matrix of constants which gives a map $V_i^{\oplus n_i} \to V_i^{\oplus m_i}$.

Corollary 20.1.3 (Subrepresentations of completely reducible representations)

Let $V = \bigoplus V_i^{\oplus n_i}$ be completely reducible. Then any subrepresentation W of V is isomorphic to $\bigoplus V_i^{\oplus m_i}$ where $m_i \le n_i$ for each i, and the inclusion $W \hookrightarrow V$ is given by the direct sum of inclusion $V_i^{\oplus m_i} \hookrightarrow V_i^{\oplus n_i}$, which are $n_i \times m_i$ matrices.

Proof. Apply Schur's lemma to the inclusion $W \hookrightarrow V$. $\square$

Recall from Section 9.5 that a linear maps from a n-dimensional vector space to a m-dimensional vector space can be written as a $n \times m$ matrix. Here the situation is similar, however the matrices are made for each irrep independently, and the non-isomorphic irreps, in some sense, "doesn't talk to each other".

Remark 20.1.4 — The representation $V^{\oplus n}$ can also be viewed as n vectors of V "stacked horizontally", as we did in Example 19.3.2:

$$\begin{pmatrix} \vdots & \vdots & & \vdots \\ v_1 & v_2 & \cdots & v_n \\ \vdots & \vdots & & \vdots \end{pmatrix} \in V^{\oplus n}.$$

That way, the action is given by

$$\begin{pmatrix} \vdots & \vdots & & \vdots \\ v_1 & v_2 & \cdots & v_n \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{bmatrix} c_{11} & c_{21} & \cdots & c_{(m-1)1} & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{(m-1)1} & c_{m2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{1n} & c_{2n} & \cdots & c_{(m-1)n} & c_{mn} \end{bmatrix} \in V^{\oplus m}.$$

It may be clearer this way to see the type mismatch happening. And this also gives a natural explanation why the intertwining operators in Problem 19D* corresponds to right matrix multiplication.

§20.2 Density theorem

We are going to take advantage of the previous result to prove that finite-dimensional algebras have finitely many irreps.

Theorem 20.2.1 (Jacobson density theorem)
Let (V_1, ρ_1), ..., (V_r, ρ_r) be pairwise nonisomorphic irreps of A. Then there is a surjective map of vector spaces

$$\bigoplus_{i=1}^{r} \rho_i \colon A \twoheadrightarrow \bigoplus_{i=1}^{r} \operatorname{Mat}(V_i).$$

The right way to think about this theorem is that

Density is the "Chinese remainder theorem" for irreps of A.

Recall that in number theory, the Chinese remainder theorem tells us that given lots of "unrelated" congruences, we can find a single N which simultaneously satisfies them all. Similarly, given lots of different nonisomorphic irreps of A, this means that we can select a single $a \in A$ which induces any tuple $(\rho_1(a), \dots, \rho_r(a))$ of actions we want — a surprising result, since even the $r = 1$ case is not obvious at all!

$$\begin{tikzcd}
 & \rho_1(a) = M_1 \in \operatorname{Mat}(V_1) \\
 & \rho_2(a) = M_2 \in \operatorname{Mat}(V_2) \\
\boxed{a \in A} \arrow[ruu] \arrow[ru] \arrow[rd] & \vdots \\
 & \rho_r(a) = M_r \in \operatorname{Mat}(V_r)
\end{tikzcd}$$

This also gives us the non-obvious corollary:

Corollary 20.2.2 (Finiteness of number of representations)
Any finite-dimensional algebra A has at most $\dim A$ irreps.

Proof. If V_i are such irreps then $A \twoheadrightarrow \bigoplus_i V_i^{\oplus \dim V_i}$, hence we have the inequality $\sum (\dim V_i)^2 \le \dim A$. $\square$

Proof of density theorem. Let $V = V_1 \oplus \cdots \oplus V_r$, so A acts on $V = (V, \rho)$ by $\rho = \bigoplus_i \rho_i$. Thus by Problem 19C*, we can instead consider ρ as an *intertwining operator*

$$\rho\colon \operatorname{Reg}(A) \to \bigoplus_{i=1}^{r} \operatorname{Mat}(V_i) \cong \bigoplus_{i=1}^{r} V_i^{\oplus d_i}.$$

We will use this instead as it will be easier to work with.

First, we handle the case $r = 1$. Fix a basis $e_1, \dots, e_n$ of $V = V_1$. Assume for contradiction that the map is not surjective. Then there is a map of representations (by ρ and the isomorphism) $\operatorname{Reg}(A) \to V^{\oplus n}$ given by $a \mapsto (a \cdot e_1, \dots, a \cdot e_n)$. By hypothesis, it is not surjective: its image is a *proper* subrepresentation of $V^{\oplus n}$. Assume its image is isomorphic to $V^{\oplus m}$ for $m < n$, so by Theorem 20.1.2 there is a matrix of constants X with

$$\begin{tikzcd}
\operatorname{Reg}(A) \arrow[r] & V^{\oplus n} & V^{\oplus m} \arrow[l, hook', "X\cdot -"'] \\
a \arrow[r, mapsto] & (a \cdot e_1, \dots, a \cdot e_n) & \\
1_A \arrow[r, mapsto] & (e_1, \dots, e_n) & (v_1, \dots, v_m) \arrow[l, mapsto]
\end{tikzcd}$$

where the two arrows in the top row have the same image; hence the pre-image $(v_1, \dots, v_m)$ of $(e_1, \dots, e_n)$ can be found. But since $m < n$ we can find constants $c_1, \dots, c_n$ not all zero such that X applied to the column vector $(c_1, \dots, c_n)$ is zero:

$$\sum_{i=1}^{n} c_i e_i = \begin{bmatrix} c_1 & \dots & c_n \end{bmatrix} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} c_1 & \dots & c_n \end{bmatrix} X \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} = 0$$

contradicting the fact that e_i are linearly independent. Hence we conclude the theorem for $r = 1$.

As for $r \ge 2$, the image $\rho^{\text{img}}(A)$ is necessarily of the form $\bigoplus_i V_i^{\oplus d_i}$ (by Corollary 20.1.3) and by the above $d_i = \dim V_i$ for each i. □

Example 20.2.3 (Applying the proof of density theorem on an explicit example)

We can run through the argument on an explicit example to better understand how it works — in order to do this, we need V to be an irrep, otherwise the image of $\operatorname{Reg}(A)$ would not be isomorphic to $V^{\oplus m}$, and we will not be able to run to the end of the argument.

Let $A = \operatorname{Mat}_2(k)$, and $V \cong k^{\oplus 2}$ with the obvious action. As we know, this is an irrep.

The density theorem claims that $\rho\colon A \to \operatorname{Mat}(V)$ is surjective, which means for any $e_1, e_2 \in V$ independent, and any $w_1, w_2 \in V$, we can find $a \in A$ such that $a \cdot (e_1, e_2) = (w_1, w_2)$.

Because we're working through a counterexample, pick $e_1 = (1, 0)$, $e_2 = (2, 0)$ instead. Then, for some $w_1, w_2 \in V$, there may be no a that sends e_1 to w_1 to e_2 to w_2.

Consider the representation morphism $\operatorname{Reg}(A) \to V^{\oplus 2}$ by $a \mapsto (a \cdot e_1, a \cdot e_2)$; its image is thus $\{(v, 2v) \mid v \in V\}$, which is a subrepresentation of $V^{\oplus 2}$, isomorphic as a representation to $V^{\oplus 1} \cong V$ by

$$v \mapsto (v, 2v) = v \begin{bmatrix} 1 & 2 \end{bmatrix}.$$

Then, we can find $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in V^{\oplus 1}$, for which

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} = v \begin{bmatrix} 1 & 2 \end{bmatrix}.$$

Now, with the explicit array of numbers $\begin{bmatrix} 1 & 2 \end{bmatrix}$, it is easy to find a linear dependence on e_1 and e_2.

§20.3 Semisimple algebras

Definition 20.3.1. A finite-dimensional algebra A is **semisimple** if every finite-dimensional representation of A is completely reducible.

Theorem 20.3.2 (Semisimple algebras)
Let A be a finite-dimensional algebra. Then the following are equivalent:

(i) $A \cong \bigoplus_i \mathrm{Mat}_{d_i}(k)$ for some d_i.

(ii) A is semisimple.

(iii) $\mathrm{Reg}(A)$ is completely reducible.

Proof. (i) $\implies$ (ii) follows from using Proposition 19.3.5 to breaks any finite-dimensional representation of A into a direct sum of representations of $\mathrm{Mat}_{d_i}(k)$, then Theorem 19.6.1 shows any such representations are completely reducible. (ii) $\implies$ (iii) is tautological.

To see (iii) $\implies$ (i), we use the following clever trick. Consider

$$\mathrm{Hom}_{\mathrm{rep}}(\mathrm{Reg}(A), \mathrm{Reg}(A)).$$

On one hand, by Problem 19D*, it is isomorphic to A^{op} (A with opposite multiplication), because the only intertwining operators $\mathrm{Reg}(A) \to \mathrm{Reg}(A)$ are those of the form $- \cdot a$. On the other hand, suppose that we have set $\mathrm{Reg}(A) = \bigoplus_i V_i^{\oplus n_i}$. By Theorem 20.1.2, we have

$$A^{\mathrm{op}} \cong \mathrm{Hom}_{\mathrm{rep}}(\mathrm{Reg}(A), \mathrm{Reg}(A)) = \bigoplus_i \mathrm{Mat}_{n_i \times n_i}(k).$$

But $\mathrm{Mat}_n(k)^{\mathrm{op}} \cong \mathrm{Mat}_n(k)$ (just by transposing), so we recover the desired conclusion. □

Remark 20.3.3 — The trick of the proof above resembles Cayley's theorem (Problem 1F†), in that we make the object act on itself to get an explicit representation.

Remark 20.3.4 — We can compare this to Corollary 18.3.2. Here, any finite-dimensional representation of A is a finite-dimensional left A-module, and from the theorem above, we know that if A is semisimple, any such module can be broken down into a direct sum of irreps $V_i \cong k^{\oplus d_i}$.

Note that unlike the case where A is a PID, $k^{\oplus d_i}$ is not isomorphic to a quotient of the ring $\mathrm{Mat}_{d_i}(k)$.

In fact, if we combine the above result with the density theorem (and Corollary 20.2.2), we obtain:

Theorem 20.3.5 (Sum of squares formula)

For a finite-dimensional algebra A we have

$$\sum_i \dim(V_i)^2 \le \dim A$$

where the V_i are the irreps of A; equality holds exactly when A is semisimple, in which case

$$\operatorname{Reg}(A) \cong \bigoplus_i \operatorname{Mat}(V_i) \cong \bigoplus_I V_i^{\oplus \dim V_i}.$$

Proof. The inequality was already mentioned in Corollary 20.2.2. It is equality if and only if the map $\rho\colon A \to \bigoplus_i \operatorname{Mat}(V_i)$ is an isomorphism; this means all V_i are present. ☐

Remark 20.3.6 (Digression) — For any finite-dimensional A, the kernel of the map $\rho\colon A \to \bigoplus_i \operatorname{Mat}(V_i)$ is denoted $\operatorname{Rad}(A)$ and is the so-called **Jacobson radical** of A; it's the set of all $a \in A$ which act by zero in all irreps of A. The usual definition of "semisimple" given in books is that this Jacobson radical is trivial.

§20.4 Maschke's theorem

We now prove that the representation theory of groups is as nice as possible.

Theorem 20.4.1 (Maschke's theorem)

Let G be a finite group, and k an algebraically closed field whose characteristic does not divide $|G|$. Then $k[G]$ is semisimple.

This tells us that when studying representations of groups, all representations are completely reducible.

Proof. Consider any finite-dimensional representation (V, ρ) of $k[G]$. Given a proper subrepresentation $W \subseteq V$, our goal is to construct a supplementary G-invariant subspace W' which satisfies

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

This will show that indecomposable $\iff$ irreducible, which is enough to show $k[G]$ is semisimple.

Let $\pi\colon V \to W$ be any projection of V onto W, meaning $\pi(v) = v \iff v \in W$. We consider the *averaging* map $P\colon V \to V$ by

$$P = \frac{1}{|G|} \sum_{g \in G} \rho(g^{-1}) \circ \pi \circ \rho(g).$$

We'll use the following properties of the map:

Exercise 20.4.2. Show that the map P satisfies:

- For any $w \in W$, $P(w) = w$.

- For any $v \in V$, $P(v) \in W$.
- The map $P \colon V \to V$ is an intertwining operator.

Thus P is idempotent (it is the identity on its image W), so by Problem 9H* we have $V = \ker P \oplus \operatorname{im} P$, but both $\ker P$ and $\operatorname{im} P$ are subrepresentations as desired. □

Remark 20.4.3 — In the case where $k = \mathbb{C}$, there is a shorter proof. Suppose $B \colon V \times V \to \mathbb{C}$ is an arbitrary bilinear form. Then we can "average" it to obtain a new bilinear form

$$\langle v, w \rangle := \frac{1}{|G|} \sum_{g \in G} B(g \cdot v, g \cdot w).$$

The averaged form $\langle -, - \rangle$ is G-invariant, in the sense that $\langle v, w \rangle = \langle g \cdot v, g \cdot w \rangle$. Then, one sees that if $W \subseteq V$ is a subrepresentation, so is its orthogonal complement $W^\perp$. This implies the result.

§20.5 Example: the representations of $\mathbb{C}[S_3]$

We compute all irreps of $\mathbb{C}[S_3]$. I'll take for granted right now there are exactly three such representations (which will be immediate by the first theorem in the next chapter: we'll in fact see that the number of representations of G is exactly equal to the number of conjugacy classes of G).

Given that, if the three representations of $\mathbb{C}[S_3]$ have dimension d_1, d_2, d_3 , then we ought to have

$$d_1^2 + d_2^2 + d_3^2 = |G| = 6.$$

From this, combined with some deep arithmetic, we deduce that we should have $d_1 = d_2 = 1$ and $d_3 = 2$ or some permutation.

In fact, we can describe these representations explicitly. First, we define:

Definition 20.5.1. Let G be a group. The complex **trivial group representation** of a group G is the one-dimensional representation $\mathbb{C}_{\text{triv}} = (\mathbb{C}, \rho)$ where $g \cdot v = v$ for all $g \in G$ and $v \in \mathbb{C}$ (i.e. $\rho(g) = \text{id}$ for all $g \in G$).

Remark 20.5.2 (Warning) — The trivial representation of an *algebra* A doesn't make sense for us: we might want to set $a \cdot v = v$ but this isn't linear in A. (You *could* try to force it to work by deleting the condition $1_A \cdot v = v$ from our definition; then one can just set $a \cdot v = 0$. But even then $\mathbb{C}_{\text{triv}}$ would not be the trivial representation of $k[G]$.)

Another way to see this is that the trivial representation depends on how the k-algebra is written as a group algebra: $k[\mathbb{Z}/2\mathbb{Z}]$ has a k-algebra automorphism given by $g \mapsto -g$, where g is the generator of the group $\mathbb{Z}/2\mathbb{Z}$; however the corresponding trivial representations are different.

Then the representations are:

- The one-dimensional $\mathbb{C}_{\text{triv}}$; each $\sigma \in S_3$ acts by the identity.
- There is a nontrivial one-dimensional representation $\mathbb{C}_{\text{sign}}$ where the map $S_3 \to \mathbb{C}^\times$ is given by sending σ to the sign of σ. Thus in $\mathbb{C}_{\text{sign}}$ every $\sigma \in S_3$ acts as ± 1. Of

course, $\mathbb{C}_{\text{triv}}$ and $\mathbb{C}_{\text{sign}}$ are not isomorphic (as one-dimensional representations are never isomorphic unless the constants they act on coincide for all a, as we saw in Problem 19A†).

- Finally, we have already seen the two-dimensional representation, but now we give it a name. Define refl_0 to be the representation whose vector space is $\{(x, y, z) \mid x + y + z = 0\}$, and whose action of S_3 on it is permutation of coordinates.

> **Exercise 20.5.3.** Show that refl_0 is irreducible, for example by showing directly that no subspace is invariant under the action of S_3.

Thus V is also not isomorphic to the previous two representations.

This implies that these are all the irreps of S_3. Note that, if we take the representation V of S_3 on $k^{\oplus 3}$, we just get that $V = \text{refl}_0 \oplus \mathbb{C}_{\text{triv}}$.

§20.6 A few harder problems to think about

Problem 20A. Find all the irreps of $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$.

Problem 20B (Maschke requires $|G|$ finite)**.** Consider the representation of the group $\mathbb{R}$ on $\mathbb{C}^{\oplus 2}$ under addition by a homomorphism

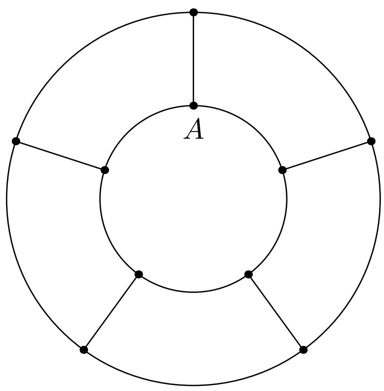
$$\mathbb{R} \to \text{Mat}_2(\mathbb{C}) \quad \text{by} \quad t \mapsto \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

Show that this representation is not irreducible, but it is indecomposable.

Problem 20C. Prove that all irreducible representations of a finite group are finite-dimensional.

Problem 20D. Determine all the complex irreps of D_{10}.

Problem 20E (AIME 2018)**.** The wheel shown below consists of two circles and five spokes, with a label where a spoke meets a circle. A bug walks along the wheel, starting from A. The bug takes 15 steps. At each step, the bug moves to an adjacent label such that it only walks counterclockwise along the inner circle and clockwise along the outer circle. In how many ways can the bug move to end up at A after all steps?



21 Characters

Characters are basically the best thing ever. To every representation V of A we will attach a so-called character $\chi_V : A \to k$. It will turn out that the characters of irreps of V will determine the representation V completely. Thus an irrep is just specified by a set of $\dim A$ numbers.

§21.1 Definitions

Definition 21.1.1. Let $V = (V, \rho)$ be a finite-dimensional representation of A. The **character** $\chi_V : A \to k$ attached to A is defined by $\chi_V = \operatorname{Tr} \circ \rho$, i.e.

$$\chi_V(a) := \operatorname{Tr}\left(\rho(a) : V \to V\right).$$

Since Tr and ρ are additive, this is a k-linear map (but it is not multiplicative). Note also that $\chi_{V \oplus W} = \chi_V + \chi_W$ for any representations V and W.

We are especially interested in the case $A = k[G]$, of course. As usual, we just have to specify $\chi_V(g)$ for each $g \in G$ to get the whole map $k[G] \to k$. Thus we often think of χ_V as a function $G \to k$, called a character of the group G. Here is the case $G = S_3$:

Example 21.1.2 (Character table of S_3)

Let's consider the three irreps of $G = S_3$ from before. For $\mathbb{C}_{\text{triv}}$ all traces are 1; for $\mathbb{C}_{\text{sign}}$ the traces are ± 1 depending on sign (obviously, for one-dimensional maps $k \to k$ the trace "is" just the map itself). For refl_0 we take a basis $(1, 0, -1)$ and $(0, 1, -1)$, say, and compute the traces directly in this basis.

$\chi_V(g)$	id	(1 2)	(2 3)	(3 1)	(1 2 3)	(3 2 1)
$\mathbb{C}_{\text{triv}}$	1	1	1	1	1	1
$\mathbb{C}_{\text{sign}}$	1	-1	-1	-1	1	1
refl_0	2	0	0	0	-1	-1

The above table is called the **character table** of the group G. The table above has certain mysterious properties, which we will prove as the chapter progresses.

(I) The value of $\chi_V(g)$ only depends on the conjugacy class of g.

(II) The number of rows equals the number of conjugacy classes.

(III) The sum of the squares of any row is 6 again!

(IV) The "dot product" of any two rows is zero.

Abuse of Notation 21.1.3. The name "character" for $\chi_V : G \to k$ is a bit of a misnomer. This χ_V is not multiplicative in any way, as the above example shows: one can almost think of it as an element of $k^{\oplus |G|}$.

> **Question 21.1.4.** Show that $\chi_V(1_A) = \dim V$, so one can read the dimensions of the representations from the leftmost column of a character table.

§21.2 The dual space modulo the commutator

For any algebra, we first observe that since $\operatorname{Tr}(TS) = \operatorname{Tr}(ST)$, we have for any V that

$$\chi_V(ab) = \chi_V(ba).$$

This explains observation (I) from earlier:

> **Question 21.2.1.** Deduce that if g and h are in the same conjugacy class of a group G, and V is a representation of $k[G]$, then $\chi(g) = \chi(h)$.

Now, given our algebra A we define the **commutator** $[A, A]$ to be the k-vector subspace spanned by $xy - yx$ for $x, y \in A$. Thus $[A, A]$ is contained in the kernel of each χ_V.

Definition 21.2.2. The space $A^{\mathrm{ab}} := A/[A, A]$ is called the **abelianization** of A. Each character of A can be viewed as a map $A^{\mathrm{ab}} \to k$, i.e. an element of $(A^{\mathrm{ab}})^\vee$.

Example 21.2.3 (Examples of abelianizations)

(a) If A is commutative, then $[A, A] = \{0\}$ and $A^{\mathrm{ab}} = A$.

(b) If $A = \operatorname{Mat}_k(d)$, then $[A, A]$ consists exactly of the $d \times d$ matrices of trace zero. (Proof: harmless exercise.) Consequently, A^{ab} is one-dimensional.

(c) Suppose $A = k[G]$. Then in A^{ab}, we identify gh and hg for each $g, h \in G$; equivalently $ghg^{-1} = h$. So in other words, A^{ab} is isomorphic to the space of k-linear combinations of the *conjugacy classes* of G.

Remark 21.2.4 (Warning) — For a group G, the abelianization of G is defined to be $G/[G, G]$, where $[G, G]$ is the subgroup generated by all the commutators.

When $A = k[G]$, the space A^{ab} is not isomorphic to the group algebra $k[G/[G, G]]$! This is because, in the abelianization of the group G, we identify $ghg^{-1}h^{-1} = 1$ for all $g, h \in G$, which is not the same as $gh - hg$.

In fact, in the general case, A^{ab} does not even inherit the structure of a k-algebra from A, it can only get a k-vector space structure.

Theorem 21.2.5 (Character of representations of algebras)

Let A be an algebra over an algebraically closed field. Then

(a) Characters of pairwise non-isomorphic irreps are linearly independent in $(A^{\mathrm{ab}})^\vee$.

(b) If A is finite-dimensional and semisimple, then the characters attached to irreps form a basis of $(A^{\mathrm{ab}})^\vee$.

In particular, in (b) the number of irreps of A equals $\dim A^{\mathrm{ab}}$.

Proof. Part (a) is more or less obvious by the density theorem: suppose there is a linear dependence, so that for every a we have

$$c_1\chi_{V_1}(a) + c_2\chi_{V_2}(a) + \cdots + c_r\chi_{V_r}(a) = 0$$

for some integer r.

Question 21.2.6. Deduce that $c_1 = \cdots = c_r = 0$ from the density theorem.

For part (b), assume there are r irreps. We may assume that

$$A = \bigoplus_{i=1}^{r} \operatorname{Mat}(V_i)$$

where $V_1, \dots, V_r$ are the irreps of A. Since we have already showed the characters are linearly independent we need only show that $\dim(A/[A,A]) = r$, which follows from the observation earlier that each $\operatorname{Mat}(V_i)$ has a one-dimensional abelianization. $\square$

Since G has $\dim k[G]^{\text{ab}}$ conjugacy classes, this completes the proof of (II).

§21.3 Orthogonality of characters

Now we specialize to the case of finite groups G, represented over $\mathbb{C}$.

Definition 21.3.1. Let $\operatorname{Classes}(G)$ denote the set of conjugacy classes of G.

If G has r conjugacy classes, then it has r irreps. Each (finite-dimensional) representation V, irreducible or not, gives a character χ_V.

Abuse of Notation 21.3.2. From now on, we will often regard χ_V as a function $G \to \mathbb{C}$ or as a function $\operatorname{Classes}(G) \to \mathbb{C}$. So for example, we will write both $\chi_V(g)$ (for $g \in G$) and $\chi_V(C)$ (for a conjugacy class C); the latter just means $\chi_V(g_C)$ for any representative $g_C \in C$.

Definition 21.3.3. Let $\operatorname{Fun}_{\text{class}}(G)$ denote the set of functions $\operatorname{Classes}(G) \to \mathbb{C}$ viewed as a vector space over $\mathbb{C}$. We endow it with the inner form

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

This is the same "dot product" that we mentioned at the beginning, when we looked at the character table of S_3. We now aim to prove the following orthogonality theorem, which will imply (III) and (IV) from earlier.

Theorem 21.3.4 (Orthogonality)
For any finite-dimensional complex representations V and W of G we have

$$\langle \chi_V, \chi_W \rangle = \dim \operatorname{Hom}_{\text{rep}}(W, V).$$

In particular, if V and W are irreps then

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & V \cong W \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 21.3.5 (Irreps give an orthonormal basis)

The characters associated to irreps form an *orthonormal* basis of $\mathrm{Fun}_{\mathrm{class}}(G)$.

In order to prove this theorem, we have to define the dual representation and the tensor representation, which give a natural way to deal with the quantity $\chi_V(g)\overline{\chi_W(g)}$.

Definition 21.3.6. Let $V = (V, \rho)$ be a representation of G. The **dual representation** $V^\vee$ is the representation on $V^\vee$ with the action of G given as follows: for each $\xi \in V^\vee$, the action of g gives a $g \cdot \xi \in V^\vee$ specified by

$$v \xmapsto{g\cdot\xi} \xi\left(\rho(g^{-1})(v)\right).$$

Definition 21.3.7. Let $V = (V, \rho_V)$ and $W = (W, \rho_W)$ be *group* representations of G. The **tensor product** of V and W is the group representation on $V \otimes W$ with the action of G given on pure tensors by

$$g \cdot (v \otimes w) = (\rho_V(g)(v)) \otimes (\rho_W(g)(w))$$

which extends linearly to define the action of G on all of $V \otimes W$.

Remark 21.3.8 — Warning: the definition for tensors does *not* extend to algebras. We might hope that $a \cdot (v \otimes w) = (a \cdot v) \otimes (a \cdot w)$ would work, but this is not even linear in $a \in A$ (what happens if we take $a = 2$, for example?).

Theorem 21.3.9 (Character traces)

If V and W are finite-dimensional representations of G, then for any $g \in G$.

(a) $\chi_{V\oplus W}(g) = \chi_V(g) + \chi_W(g)$.

(b) $\chi_{V\otimes W}(g) = \chi_V(g) \cdot \chi_W(g)$.

(c) $\chi_{V^\vee}(g) = \overline{\chi_V(g)}$.

Proof. Parts (a) and (b) follow from the identities $\mathrm{Tr}(S \oplus T) = \mathrm{Tr}(S) + \mathrm{Tr}(T)$ and $\mathrm{Tr}(S \otimes T) = \mathrm{Tr}(S)\,\mathrm{Tr}(T)$. However, part (c) is trickier. As $(\rho(g))^{|G|} = \rho(g^{|G|}) = \rho(1_G) = \mathrm{id}_V$ by Lagrange's theorem, we can diagonalize $\rho(g)$, say with eigenvalues $\lambda_1, \dots, \lambda_n$ which are $|G|$th roots of unity, corresponding to eigenvectors $e_1, \dots, e_n$. Then we see that in the basis $e_1^\vee, \dots, e_n^\vee$, the action of g on $V^\vee$ has eigenvalues $\lambda_1^{-1}, \lambda_2^{-1}, \dots, \lambda_n^{-1}$. So

$$\chi_V(g) = \sum_{i=1}^n \lambda_i \quad \text{and} \quad \chi_{V^\vee}(g) = \sum_{i=1}^n \lambda_i^{-1} = \sum_{i=1}^n \overline{\lambda_i}$$

where the last step follows from the identity $|z| = 1 \iff z^{-1} = \overline{z}$. $\square$

Remark 21.3.10 (Warning) — The identities (b) and (c) do not extend linearly to $\mathbb{C}[G]$, i.e. it is not true for example that $\chi_{V^\vee}(a) = \overline{\chi_V(a)}$ if we think of χ_V as a map $\mathbb{C}[G] \to \mathbb{C}$.

Proof of orthogonality relation. The key point is that we can now reduce the sums of products to just a single character by

$$\chi_V(g)\overline{\chi_W(g)} = \chi_{V\otimes W^\vee}(g).$$

So we can rewrite the sum in question as just

$$\langle \chi_V, \chi_W \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_{V\otimes W^\vee}(g) = \chi_{V\otimes W^\vee}\left(\frac{1}{|G|}\sum_{g\in G} g\right).$$

Let $P\colon V\otimes W^\vee \to V\otimes W^\vee$ be the action of $\frac{1}{|G|}\sum_{g\in G} g$, so we wish to find $\operatorname{Tr} P$.

Exercise 21.3.11. Show that P is idempotent. (Compute $P\circ P$ directly.)

Hence $V\otimes W^\vee = \ker P \oplus \operatorname{im} P$ (by Problem 9H*) and $\operatorname{im} P$ is the subspace of elements which are fixed under G. From this we deduce that

$$\operatorname{Tr} P = \dim \operatorname{im} P = \dim\left\{x \in V\otimes W^\vee \mid g\cdot x = x \ \forall g \in G\right\}.$$

Now, consider the natural isomorphism $V\otimes W^\vee \to \operatorname{Hom}(W,V)$.

Exercise 21.3.12. Let $g\in G$. Show that under this isomorphism, $T\in\operatorname{Hom}(W,V)$ satisfies $g\cdot T = T$ if and only if $T(g\cdot w) = g\cdot T(w)$ for each $w\in W$. (This is just unwinding three or four definitions.)

Consequently, $\chi_{V\otimes W^\vee}(P) = \operatorname{Tr} P = \dim \operatorname{Hom}_{\text{rep}}(W,V)$ as desired. □

The orthogonality relation gives us a fast and mechanical way to check whether a finite-dimensional representation V is irreducible. Namely, compute the traces $\chi_V(g)$ for each $g\in G$, and then check whether $\langle\chi_V,\chi_V\rangle = 1$. So, for example, we could have seen the three representations of S_3 that we found were irreps directly from the character table. Thus, we can now efficiently verify any time we have a complete set of irreps.

§21.4 Examples of character tables

Example 21.4.1 (Dihedral group on 10 elements)

Let $D_{10} = \langle r, s \mid r^5 = s^2 = 1, rs = sr^{-1}\rangle$. Let $\omega = \exp(\frac{2\pi i}{5})$. We write four representations of D_{10}:

- $\mathbb{C}_{\text{triv}}$, all elements of D_{10} act as the identity.
- $\mathbb{C}_{\text{sign}}$, r acts as the identity while s acts by negation.
- V_1, which is two-dimensional and given by $r \mapsto \begin{bmatrix}\omega & 0\\ 0 & \omega^4\end{bmatrix}$ and $s\mapsto \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$.
- V_2, which is two-dimensional and given by $r \mapsto \begin{bmatrix}\omega^2 & 0\\ 0 & \omega^3\end{bmatrix}$ and $s\mapsto \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$.

We claim that these four representations are irreducible and pairwise non-isomorphic.

We do so by writing the character table:

D_{10}	1	r, r^4	r^2, r^3	sr^k
$\mathbb{C}_{\text{triv}}$	1	1	1	1
$\mathbb{C}_{\text{sign}}$	1	1	1	-1
V_1	2	$\omega + \omega^4$	$\omega^2 + \omega^3$	0
V_2	2	$\omega^2 + \omega^3$	$\omega + \omega^4$	0

Then a direct computation shows the orthogonality relations, hence we indeed have an orthonormal basis. For example, $\langle \mathbb{C}_{\text{triv}}, \mathbb{C}_{\text{sign}} \rangle = 1 + 2 \cdot 1 + 2 \cdot 1 + 5 \cdot (-1) = 0$.

Example 21.4.2 (Character table of S_4)

We now have enough machinery to compute the character table of S_4, which has five conjugacy classes (corresponding to cycle types id, 2, 3, 4 and $2+2$). First of all, we note that it has two one-dimensional representations, $\mathbb{C}_{\text{triv}}$ and $\mathbb{C}_{\text{sign}}$, and these are the only ones (because there are only two homomorphisms $S_4 \to \mathbb{C}^\times$). So thus far we have the table

S_4	1	$(\bullet\,\bullet)$	$(\bullet\,\bullet\,\bullet)$	$(\bullet\,\bullet\,\bullet\,\bullet)$	$(\bullet\,\bullet)(\bullet\,\bullet)$
$\mathbb{C}_{\text{triv}}$	1	1	1	1	1
$\mathbb{C}_{\text{sign}}$	1	-1	1	-1	1
$\vdots$			$\vdots$		

Note the columns represent $1 + 6 + 8 + 6 + 3 = 24$ elements.

Now, the remaining three representations have dimensions d_1, d_2, d_3 with

$$d_1^2 + d_2^2 + d_3^2 = 4! - 2 = 22$$

which has only $(d_1, d_2, d_3) = (2, 3, 3)$ and permutations. Now, we can take the refl_0 representation

$$\{(w, x, y, z) \mid w + x + y + z = 0\}$$

with basis $(1, 0, 0, -1)$, $(0, 1, 0, -1)$ and $(0, 0, 1, -1)$. This can be geometrically checked to be irreducible, but we can also do this numerically by computing the character directly (this is tedious): it comes out to have 3, 1, 0, -1, -1 which indeed gives norm

$$\langle \chi_{\text{refl}_0}, \chi_{\text{refl}_0} \rangle = \frac{1}{4!}\left(\underbrace{3^2}_{\text{id}} + \underbrace{6 \cdot (1)^2}_{(\bullet\,\bullet)} + \underbrace{8 \cdot (0)^2}_{(\bullet\,\bullet\,\bullet)} + \underbrace{6 \cdot (-1)^2}_{(\bullet\,\bullet\,\bullet\,\bullet)} + \underbrace{3 \cdot (-1)^2}_{(\bullet\,\bullet)(\bullet\,\bullet)} \right) = 1.$$

Note that we can also tensor this with the sign representation, to get another irreducible representation (since $\mathbb{C}_{\text{sign}}$ has all traces ± 1, the norm doesn't change). Finally, we recover the final row using orthogonality (which we name $\mathbb{C}^2$, for lack of a better name); hence the completed table is as follows.

S_4	1	$(\bullet\,\bullet)$	$(\bullet\,\bullet\,\bullet)$	$(\bullet\,\bullet\,\bullet\,\bullet)$	$(\bullet\,\bullet)(\bullet\,\bullet)$
$\mathbb{C}_{\text{triv}}$	1	1	1	1	1
$\mathbb{C}_{\text{sign}}$	1	-1	1	-1	1
$\mathbb{C}^2$	2	0	-1	0	2
refl_0	3	1	0	-1	-1
$\text{refl}_0 \otimes \mathbb{C}_{\text{sign}}$	3	-1	0	1	-1

§21.5 A few harder problems to think about

Problem 21A† (Reading decompositions from characters)**.** Let W be a complex representation of a finite group G. Let $V_1, \dots, V_r$ be the complex irreps of G and set $n_i = \langle \chi_W, \chi_{V_i} \rangle$. Prove that each n_i is a non-negative integer and

$$W = \bigoplus_{i=1}^{r} V_i^{\oplus n_i}.$$

Problem 21B. Consider complex representations of $G = S_4$. The representation $\text{refl}_0 \otimes \text{refl}_0$ is 9-dimensional, so it is clearly reducible. Compute its decomposition in terms of the five irreducible representations.

Problem 21C (Tensoring by one-dimensional irreps)**.** Let V and W be irreps of G, with $\dim W = 1$. Show that $V \otimes W$ is irreducible.

Problem 21D (Quaternions)**.** Compute the character table of the quaternion group Q_8.

Problem 21E* (Second orthogonality formula)**.** Let g and h be elements of a finite group G, and let $V_1, \dots, V_r$ be the irreps of G. Prove that

$$\sum_{i=1}^{r} \chi_{V_i}(g)\overline{\chi_{V_i}(h)} = \begin{cases} |C_G(g)| & \text{if } g \text{ and } h \text{ are conjugates} \\ 0 & \text{otherwise.} \end{cases}$$

Here, $C_G(g) = \{x \in G : xg = gx\}$ is the centralizer of g.

22 Some applications

With all this setup, we now take the time to develop some nice results which are of independent interest.

§22.1 Frobenius divisibility

Theorem 22.1.1 (Frobenius divisibility)

Let V be a complex irrep of a finite group G. Then $\dim V$ divides $|G|$.

The proof of this will require algebraic integers (developed in the algebraic number theory chapter). Recall that an *algebraic integer* is a complex number which is the root of a monic polynomial with integer coefficients, and that these algebraic integers form a ring $\overline{\mathbb{Z}}$ under addition and multiplication, and that $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

First, we prove:

Lemma 22.1.2 (Elements of $\mathbb{Z}[G]$ are integral)

Let $\alpha \in \mathbb{Z}[G]$. Then there exists a monic polynomial P with integer coefficients such that $P(\alpha) = 0$.

Proof. Let A_k be the $\mathbb{Z}$-span of $1, \alpha^1, \dots, \alpha^k$. Since $\mathbb{Z}[G]$ is Noetherian, the inclusions $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$ cannot all be strict, hence $A_k = A_{k+1}$ for some k, which means α^{k+1} can be expressed in terms of lower powers of α. □

Proof of Frobenius divisibility. Let C_1, ..., C_m denote the conjugacy classes of G. Then consider the rational number

$$\frac{|G|}{\dim V};$$

we will show it is an algebraic integer, which will prove the theorem. Observe that we can rewrite it as

$$\frac{|G|}{\dim V} = \frac{|G| \left< \chi_V, \chi_V \right>}{\dim V} = \sum_{g \in G} \frac{\chi_V(g)\overline{\chi_V(g)}}{\dim V}.$$

We split the sum over conjugacy classes, so

$$\frac{|G|}{\dim V} = \sum_{i=1}^{m} \overline{\chi_V(C_i)} \cdot \frac{|C_i|\chi_V(C_i)}{\dim V}.$$

We claim that for every i,

$$\frac{|C_i|\chi_V(C_i)}{\dim V} = \frac{1}{\dim V} \operatorname{Tr} T_i$$

is an algebraic integer, where

$$T_i := \rho\left(\sum_{h \in C_i} h\right).$$

To see this, note that T_i commutes with elements of G, and hence is an intertwining operator $T_i \colon V \to V$. Thus by Schur's lemma, $T_i = \lambda_i \cdot \mathrm{id}_V$ and $\operatorname{Tr} T = \lambda_i \dim V$. By Lemma 22.1.2, $\lambda_i \in \overline{\mathbb{Z}}$, as desired.

Now we are done, since $\overline{\chi_V(C_i)} \in \overline{\mathbb{Z}}$ too (it is the sum of conjugates of roots of unity), so $\frac{|G|}{\dim V}$ is the sum of products of algebraic integers, hence itself an algebraic integer. □

§22.2 Burnside's theorem

We now prove a group-theoretic result. This is the famous poster child for representation theory (in the same way that RSA is the poster child of number theory) because the result is purely group theoretic.

Recall that a group is **simple** if it has no normal subgroups. In fact, we will prove:

Theorem 22.2.1 (Burnside)

Let G be a nonabelian group of order $p^a q^b$ (where p, q are distinct primes and $a, b \ge 0$). Then G is not simple.

In what follows p and q will always denote prime numbers.

Lemma 22.2.2 (On $\gcd(|C|, \dim V) = 1$)

Let $V = (V, \rho)$ be an complex irrep of G. Assume C is a conjugacy class of G with $\gcd(|C|, \dim V) = 1$. Then for any $g \in C$, either

- $\rho(g)$ is multiplication by a scalar, or
- $\chi_V(g) = \operatorname{Tr} \rho(g) = 0$.

Proof. If ε_i are the n eigenvalues of $\rho(g)$ (which are roots of unity), then from the proof of Frobenius divisibility we know $\frac{|C|}{n} \chi_V(g) \in \overline{\mathbb{Z}}$, thus from $\gcd(|C|, n) = 1$ we get

$$\frac{1}{n} \chi_V(g) = \frac{1}{n}(\varepsilon_1 + \cdots + \varepsilon_n) \in \overline{\mathbb{Z}}.$$

So this follows readily from a fact from algebraic number theory, namely Problem 53C*: either $\varepsilon_1 = \cdots = \varepsilon_n$ (first case) or $\varepsilon_1 + \cdots + \varepsilon_n = 0$ (second case). □

Lemma 22.2.3 (Simple groups don't have prime power conjugacy classes)

Let G be a finite simple group. Then G cannot have a conjugacy class of order p^k (where $k > 0$).

Proof. By contradiction. Assume C is such a conjugacy class, and fix any $g \in C$. By the second orthogonality formula (Problem 21E*) applied g and 1_G (which are not conjugate since $g \ne 1_G$) we have

$$\sum_{i=1}^{r} \dim V_i \chi_{V_i}(g) = 0$$

where V_i are as usual all irreps of G.

Exercise 22.2.4. Show that there exists a nontrivial irrep V such that $p \nmid \dim V$ and $\chi_V(g) \neq 0$. (Proceed by contradiction to show that $-\frac{1}{p} \in \overline{\mathbb{Z}}$ if not.)

Let $V = (V, \rho)$ be the irrep mentioned. By the previous lemma, we now know that $\rho(g)$ acts as a scalar in V.

Now consider the subgroup

$$H = \left\langle ab^{-1} \mid a, b \in C \right\rangle \subseteq G.$$

We claim this is a nontrivial normal subgroup of G. It is easy to check H is normal, and since $|C| > 1$ we have that H is nontrivial. As represented by V each element of H acts trivially in G, so since V is nontrivial and irreducible, $H \neq G$. This contradicts the assumption that G was simple. □

With this lemma, Burnside's theorem follows by partitioning the $|G|$ elements of our group into conjugacy classes. Assume for contradiction G is simple. Each conjugacy class must have order either 1 (of which there are $|Z(G)|$ by Problem 16D*) or divisible by pq (by the previous lemma), but on the other hand the sum equals $|G| = p^a q^b$. Consequently, we must have $|Z(G)| > 1$. But G is not abelian, hence $Z(G) \neq G$, thus the center $Z(G)$ is a nontrivial normal subgroup, contradicting the assumption that G was simple.

§22.3 Frobenius determinant

We finish with the following result, the problem that started the branch of representation theory. Given a finite group G, we create n variables $\{x_g\}_{g \in G}$, and an $n \times n$ matrix M_G whose (g, h)th entry is x_{gh}.

Example 22.3.1 (Frobenius determinants)

(a) If $G = \mathbb{Z}/2\mathbb{Z} = \langle T \mid T^2 = 1 \rangle$ then the matrix would be

$$M_G = \begin{bmatrix} x_{\mathrm{id}} & x_T \\ x_T & x_{\mathrm{id}} \end{bmatrix}.$$

Then $\det M_G = (x_{\mathrm{id}} - x_T)(x_{\mathrm{id}} + x_T)$.

(b) If $G = S_3$, a long computation gives the irreducible factorization of $\det M_G$ is

$$\left(\sum_{\sigma \in S_3} x_\sigma \right) \left(\sum_{\sigma \in S_3} \operatorname{sign}(\sigma) x_\sigma \right) \left(F\left(x_{\mathrm{id}}, x_{(123)}, x_{(321)}\right) - F\left(x_{(12)}, x_{(23)}, x_{(31)}\right) \right)^2$$

where $F(a, b, c) = a^2 + b^2 + c^2 - ab - bc - ca$; the latter factor is irreducible.

Theorem 22.3.2 (Frobenius determinant)

The polynomial $\det M_G$ (in $|G|$ variables) factors into a product of irreducible polynomials such that

(i) The number of polynomials equals the number of conjugacy classes of G, and

(ii) The multiplicity of each polynomial equals its degree.

You may already be able to guess how the "sum of squares" result is related! (Indeed, look at $\deg\det M_G$.)

Legend has it that Dedekind observed this behavior first in 1896. He didn't know how to prove it in general, so he sent it in a letter to Frobenius, who created representation theory to solve the problem.

With all the tools we've built, it is now fairly straightforward to prove the result.

Proof. Let $V = (V, \rho) = \operatorname{Reg}(\mathbb{C}[G])$ and let $V_1, \dots, V_r$ be the irreps of G. Let's consider the map $T \colon \mathbb{C}[G] \to \mathbb{C}[G]$ which has matrix M_G in the usual basis of $\mathbb{C}[G]$, namely

$$T \colon T(\{x_g\}_{g\in G}) = \sum_{g\in G} x_g \rho(g) \in \operatorname{Mat}(V).$$

Thus we want to examine $\det T$.

But we know that $V = \bigoplus_{i=1}^r V_i^{\oplus \dim V_i}$ as before, and so breaking down T over its subspaces we know

$$\det T = \prod_{i=1}^r \left(\det(T\restriction_{V_i})\right)^{\dim V_i}.$$

So we only have to show two things: the polynomials $\det T_{V_i}$ are irreducible, and they are pairwise different for different i.

Let $V_i = (V_i, \rho)$, and pick $k = \dim V_i$.

- *Irreducible*: By the density theorem, for any $M \in \operatorname{Mat}(V_i)$ there exists a *particular* choice of complex numbers $x_g \in G$ such that

  $$M = \sum_{g\in G} x_g \cdot \rho_i(g) = (T\restriction_{V_i})(\{x_g\}).$$

  View $\rho_i(g)$ as a $k \times k$ matrix with complex coefficients. Thus the "generic" $(T\restriction_{V_i})(\{x_g\})$, viewed as a matrix with polynomial entries, must have linearly independent entries (or there would be some matrix in $\operatorname{Mat}(V_i)$ that we can't achieve).

  Then, the assertion follows (by a linear variable change) from the simple fact that the polynomial $\det(y_{ij})_{1\le i,j\le m}$ in m^2 variables is always irreducible.

- *Pairwise distinct*: We show that from $\det T|_{V_i}(\{x_g\})$ we can read off the character χ_{V_i}, which proves the claim. In fact

  > **Exercise 22.3.3.** Pick *any* basis for V_i. If $\dim V_i = k$, and $1_G \neq g \in G$, then
  >
  > $$\chi_{V_i}(g) \text{ is the coefficient of } x_g x_{1_G}^{k-1}.$$

  Thus, we are done. □