Representation Theory

Summary by Ari Feiglin (ari.feiglin@gmail.com)

Contents

1 Basic Representation Theory

1.1 Group actions

We recall that we can view a group action of a group G on a set X equivalently as either a group homomorphism $\rho: G \to S_X$, or as a map $\cdot: G \times X \to X$ (written as juxtaposition) where

(1) $ex = x$,

(2) $g_1(g_2x) = (g_1g_2)x$

The relation between these two equivalent definitions is $\rho(g)(x) = gx$. A group action is also called a **G-set**.

1.1.1 Example

Consider a finite-dimensional vector space V. Then the group of automorphisms over V (denoted $\mathrm{GL}(V)$) acts on V in the obvious way.

If we further assume that V is an inner product space, then let $S = \{v \in V \mid |v| = 1\}$ and let $O(V)$ be the group of orthonormal automorphisms (those which preserve the inner product). Then $O(V)$ acts on S again in the obvious way. Note that $\mathrm{GL}(V)$ acts on V the same way that $O(V)$ acts on S.

1.1.2 Example

Let $H \subseteq G$ be a subgroup (not necessarily normal). Then G/H (the set of cosets) can be made into a G-set by defining $g(g'H) = (gg')H$.

1.1.3 Definition

Let X and Y be G-sets. Then a **morphism of G-sets** $X \to Y$ is a function $f: X \to Y$ satisfying $f(gx) = gf(x)$ for all $g \in G$, $x \in X$.

This definition of morphisms of G-sets, along with the usual composition, makes the class of G-sets into a category. We denote this category by Set$G$ (or Set_G), and similarly denote the hom-set of morphisms as $\mathrm{Set}_G(X, Y)$.

Recall that a transitive group action is one where for every $x_1, x_2 \in X$ there exists a $g \in G$ such that $gx_1 = x_2$.

1.1.4 Example

Let G act on X transitively. Let $x_0 \in X$ and define

$$\mathrm{Stab}_G(x_0) = \{g \in G \mid gx_0 = x_0\}$$

the **stabilizer** of x_0. The stabilizer is clearly a subgroup of G, and we have a natural isomorphism of G-sets $G/\mathrm{Stab}_G(x_0) \cong X$.

1.1.5 Example

Notice that $O(V)$ acts transitively on S (this is a simple result of linear algebra). Let $s_0 \in S$, and define W to be the orthogonal complement of s_0. Then notice that $\mathrm{Stab}_{O(V)}(s_0)$ is naturally isomorphic to $O(W)$ (since an orthonormal automorphism of W can be uniquely extended to an orthonormal automorphism of

V with s_0 as a fixed point).

By the above example, we have that

$$O(V)/\mathrm{Stab}_{O(V)}(s_0) \cong S$$

We can thus abuse notation and write $O(V)/O(W) \cong S$ (viewing $O(W)$ as a subgroup of $O(V)$). Writing $O(n)$ for $O(V)$ when $n = \dim V$, we thus have $O(n)/O(n-1) \cong S^n$.

1.2 Representations

1.2.1 Definition

Given a group G, a **representation of** G (or a G**-representation**), is a group homomorphism $\rho: G \to \mathrm{GL}(V)$ (where V is a vector space over some given field). ρ is usually kept implicit, so instead of writing $\rho(g)v$ for example, we write gv.

Given two G-representations $rho_1: G \to \mathrm{GL}(V_1)$ and $\rho_2: G \to \mathrm{GL}(V_2)$, a morphism $\rho_1 \to \rho_2$ is a linear morphism $T: V_1 \to V_2$ such that $T(\rho_1(g)v) = \rho_2(g)(Tv)$ (i.e. $Tgv = gTv$).

We denote the space of linear morphisms $V \to W$ by $\hom(V, W)$, and of G-representations by $\hom_G(V, W)$ (which is a subspace of $\hom(V, W)$).

1.2.2 Example

$\mathbb{F}^n$ can be made into a representation of S_n by defining

$$\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}1} \\ \vdots \\ x_{\sigma^{-1}n} \end{pmatrix}$$

1.2.3 Example

In general, consider the space of (pure) functions $X \to \mathbb{F}$ $\mathrm{Set}(X, \mathbb{F})$ where X is a G-set. This can be made into a representation of G by setting

$$(gf)(x) = f(g^{-1}x)$$

Consider then the $\mathbb{F}$-vector space $\mathbb{F}[X]$ (which is the space obtained by taking formal linear combinations of symbols $x \in X$). Then $\mathbb{F}[X]$ can be made into a G-representation where x is mapped to gx (this uniquely extends to all of $\mathbb{F}[X]$).

Now, when X is finite, we have that $\mathrm{Set}(X, \mathbb{F}) \cong \mathbb{F}[X]$ naturally (as vector spaces). If X is a G-set, this is an isomorphism of G-representations.

Let V be an $\mathbb{F}$-vector space, and G a group. Then the **trivial representation** of G is the representation which maps each $g \in G$ to the identity morphism.

1.2.4 Example

A **character** is a group morphism $\chi: G \to \mathbb{F}^\times$. Given a character, we can make $\mathbb{F}$ a G-representation by

defining

$$gc = \chi(g)c$$

We denote this representation by $\mathbb{F}_\chi$. This is indeed a representation: $\mathbb{F}_\chi(g)$ is clearly in $\mathrm{GL}(\mathbb{F})$ for each $g \in G$, and $\mathbb{F}_\chi(gh)c = \chi(g)\chi(h)c = \mathbb{F}_\chi(g)\chi(h)c = \mathbb{F}_\chi(g)\mathbb{F}_\chi(h)c$.

1.2.5 Definition

Let V be a G-representation, and W a subspace of V. Then W is a **G-subrepresentation** of V if it is invariant: $gw \in W$ for all $w \in W$. We can then naturally view W as a G-representation in and of itself.

1.2.6 Definition

Let V be a G-representation and W a G-subrepresentation. Then V/W forms a G-representation, called the **quotient G-representation** defined by $g(v + W) = gv + W$. This is well-defined precisely because W is a G-subrepresentation.

1.2.7 Definition

A G-representation V is **irreducible** (or **simple**) if $V \neq 0$ and it has no non-trivial G-subrepresentations (meaning that every G-subrepresentation is either V or 0). V is **indecomposable** if V is non-trivial and when $V = W_1 \oplus W_2$ then the direct summands are trivial (i.e. $W_1 = V$ or 0).

Clearly an irreducible representation is indecomposable. We will later see that when the characteristic of the underlying field is zero, the converse is true.

1.2.8 Example (An indecomposable representation which is not irreducible)

Let us consider S_2 acting on $\mathbb{F}^2$ as above, where $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$. Then $\mathbb{F}^2$ is not an irreducible S_2-representation, since $W = \{(x_1, x_2) \mid x_1 + x_2 = 0\}$ is a S_2-subrepresentation of $\mathbb{F}^2$ which is non-trivial. However, $\mathbb{F}^2$ is an indecomposable S_2-representation.

For let $\mathbb{F}^2 = W_1 \oplus W_2$, then W_1, W_2 must have dimension 1, let L have dimension 1. Since linear automorphisms of L must be scalar multiplications, $(1\ 2) \in S_2$ acts as scalar multiplication. But since the only non-zero scalar in the field is 1, S_2 acts trivialy on L.

Then S_2 acts trivially on W_1, W_2, and thus trivially on all of $\mathbb{F}^2$. But $(1\ 2)$ does not act trivially on all of $\mathbb{F}^2$, in contradiction.

1.3 Semisimple representations

The **direct sum** of two G-representations V_1 and V_2 is constructed over their direct sum as vector spaces $V_1 \oplus V_2$ where $g(v_1, v_2) = (gv_1, gv_2)$.

1.3.1 Proposition

Let V_1, V_2 be G-representations, and $T\colon V_1 \to V_2$ be a morphism of G-representations. Then the kernel of T is a G-subrepresentation of V_1, and the image of T is a G-subrepresentation of V_2. Furthermore, the **cokernel** $\mathrm{coker}T$, defined to be $V_2/\mathrm{im}T$, is a G-representation.

1.3.2 Definition

A G-representation V is **semisimple** if for every G-subrepresentation $W \subseteq V$, there exists another G-subrepresentation $W' \subseteq V$ such that $V = W \oplus W'$.

1.3.3 Theorem (Maschke's Theorem)

Let G be a finite group, and $\mathbb{F}$ a field whose characteristic does not divide the order of G. Then every finite-dimensional G-representation is semisimple.

We give two distinct proofs of Maschke's theorem.

Proof (first proof)

Let V be a finite-dimensional G-representation, where ρ is the representation, and let $W \subseteq V$ be a G-subrepresentation. Since V is finite-dimensional, there exists a complementary subspace $W' \subseteq V$ where $V = W \oplus W'$. We now consider the projection operator of W along W': i.e. $P(w + w') = w$. We define the endomorphism $Q\colon V \to V$:

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

We claim that Q is a projection operator of W. First we note that Q is the identity on W: since $\rho(g)^{-1}(w) = \rho(g^{-1})(w) \in W$ we have that $\rho(g)P\rho(g^{-1})(w) = \rho(g)\rho(g^{-1})(w) = w$. And so

$$Qw = \frac{1}{|G|} \sum_{g \in G} w = w$$

as required. Now we note that the image of Q is contained within W. This is simply because the image of P is W, and ρ preserves W. Thus Q is a projection operator of W (where $V = W \oplus \ker Q$).

Now we claim that Q is a morphism of G-representations: for $h \in G$ we must show that $Q \circ \rho(h) = \rho(h) \circ Q$. Indeed:

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

substituting $h^{-1}g$ for g in the sum gives

$$\frac{1}{|G|} \sum_{g \in G} \rho(hg) \circ P \circ \rho(g^{-1}) = \frac{1}{|G|}\rho(h) \sum_{g \in G} \rho(g) \circ P \circ \rho(g^{-1}) = \rho(h) \circ Q$$

as required.

So $Q\colon V \to V$ is a morphism of G-representations and a projection operator of W. Since it is a morphism of G-representations, $\ker Q$ is a G-subrepresentation. And as noted, this is a complementary subspace of W, as required. ■

Let us take a moment to internalize a few parts of this proof.

1.3.4 Definition

Let V and W be G-representations. On $\hom(V, W)$ (not just $\hom_G(V, W)$) we define the structure of a G-representation by defining

$$(g\phi)(v) = g\phi(g^{-1}v)$$

(The representation maps g to an automorphism of $\hom(V, W)$, i.e. we must map ϕ to another morphism in $\hom(V, W)$.) We also denote $g\phi$ by $g \star \phi$, to note confuse it with $\rho(g) \circ \phi$. So $g \star \phi = \rho(g) \circ \phi \circ \rho(g)^{-1}$.

This is indeed a representation: $g \star \phi$ is clearly linear so $g \star \phi \in \hom(V, W)$. Now, $\phi \mapsto g \star \phi$ is itself an automorphism of $\hom(V, W)$: it is clearly a bijection, and it is similarly clearly linear. Now let us consider the representation itself $R\colon G \to \mathrm{GL}(\hom(V, W))$, $R(g)(\phi) = g \star \phi$. This must be a group homomorphism: $R(gh) = R(g) \circ R(h)$. Indeed: $R(g) \circ R(h)(\phi) = R(g)(h \star \phi) = g \star (h \star \phi) = (gh) \star \phi = R(gh)(\phi)$ as required.

1.3.5 Definition

Let V be a G-representation, define the G-subrepresentation of **invariants** to be

$$V^G = \{v \in V \mid \text{for all } g \in G,\ gv = v\}$$

This is indeed a subspace, since $\rho(g)$ is linear, and it is a subrepresentation since $g(hv) = (gh)v = v$.

1.3.6 Definition

Let V be a G-representation, and suppose that the characteristic of $\mathbb{F}$ does not divide $|G|$ (so that $|G| \neq 0$ and is therefore invertible). Define the **averaging operator** $\mathrm{Av}_V^G\colon V \to V$ to be

$$\mathrm{Av}_V^G(v) = \frac{1}{|G|} \sum_{g \in G} gv$$

Note that Av_V^G is a projection operator on V^G: clearly it is the identity on V^G, and its image is contained in V^G.

Now, notice that $T \in \hom(V, W)$ is a morphism of G-representations if and only if $g \star T = T$ for all $g \in G$. Indeed, $g \star T = \rho(g) \circ T \circ \rho(g)^{-1}$, and this is always T if and only if T commutes with all $\rho(g)$, i.e. is a morphism. Thus

$$\hom_G(V, W) = \hom(V, W)^G$$

So in our above proof, we consider the G-representation $\hom(V, V)$ and an element $P \in \hom(V, V)$. We then define $Q = \mathrm{Av}^G_{\hom(V,V)}(P)$, and so $Q \in \hom(V, V)^G = \hom_G(V, V)$. And we further showed that P being a projection implies Q being a projection.

Proof (second proof)

Consider the projection $\pi\colon V \to V/W$. We want to show the existence of a G-morphism $\iota\colon V/W \to V$ such that $\pi \circ \iota = \mathrm{id}_{V/W}$. Then the image of ι would be complementary to W, and would be a G-subrepresentation.

More generally, given a surjective morphism of G-representations $\pi\colon V \to Z$, and a G-representation U we would like to show that $\pi_*\colon \hom_G(U, V) \to \hom_G(U, Z)$ (post composition with π) is surjective. This map is the restriction of the more general $\pi_*\colon \hom(U, V) \to \hom(U, Z)$. This map is clearly surjective and a morphism of G-representations.

So now we recast the problem as follows: given G-representations V and W and a sujective G-morphism $p\colon V \to W$, the restricted morphism $p\colon V^G \to W^G$ is surjective as well. Indeed: given $w \in W^G$ let $v \in V$ such that $pv = w$, then $p(\mathrm{Av}_V^G(v)) = \mathrm{Av}_V^G(p(v)) = \mathrm{Av}_V^G(w) = w$, so $\mathrm{Av}_V^G(v)$ is in the preimage of w under the restricted p. ■

1.4 Decomposition into irreducibles

We will assume in this section that G is a finite group and $\mathbb{F}$'s characteristic does not divide G's order.

1.4.1 Lemma

Let V be a finite-dimensional G-representation. Then there exist irreducible G-representations $E_1, \ldots, E_n$ such that V is isomorphic to $E_1 \oplus \cdots \oplus E_n$ as G-representations.

Proof

We induct on the dimension of V. If $\dim V = 0$, then an empty sum suffices. If V is itself irreducible, then $E_1 = V$ works. Otherwise, let W be a non-trivial subrepresentation of V. By Maschke's theorem, V is semisimple and therefore there exists a subrepresentation W' such that $V = W \oplus W'$. By induction, both of these subrepresentations are isomorphic to the direct sum of irreducible G-representations. Then V is isomorphic to the direct sum of these direct sums, itself a direct sum. ■

1.4.2 Lemma (Schur's Lemma)

Let E and F be irreducible G-representations. Then a morphism between them is either trivial or an isomorphism.

Proof

Let $T\colon E \to F$ be a non-trivial morphism of G-representations. Since T is non-trivial, $\ker T$ mustn't be all of E, and since E is irreducible this means that $\ker T$ must be trivial. So T is injective. Similarly, consider $\mathrm{im} T$, which cannot be trivial and therefore (since F is irreducible) must be all of F. So T is surjective. Therefore, T is an isomorphism. ■

1.4.3 Proposition

An irreducible G-representation (when G is finite), is finite-dimensional.

Proof

Let V be an infinite-dimensional G-representation. Take $v \in V$ non-zero, and define $W = \mathrm{span}\{gv\}_{g\in G}$. Since $v \in W$, it is non-zero, and because it is spanned by a finite set W is not all of V. And furthermore W is clearly a G-representation. ■

1.4.4 Lemma

Let V be finite-dimensional, and $V \cong E_1 \oplus \cdots \oplus E_n \cong F_1 \oplus \cdots \oplus F_m$ be irreducible factorizations of V. Then for every irreducible G-representation E, the number of E_i isomorphic to E is equal the number of F_i isomorphic to E, both being $\dim \hom_G(V,E)/\dim \hom_G(E,E)$.

Proof

Let $d = \hom_G(E,E)$, and $d \geq 1$ as $\hom_G(E,E)$ is non-trivial (the identity). By Schur's lemma, for an irreducible G-representation F, $\dim_G(E,F) = 0$ if F is not isomorphic to E. Thus:

$$\dim \hom_G(V,E) = \dim \hom_G(E_1 \oplus \cdots \oplus E_n, E) = \dim \hom_G(E_1,E) + \cdots + \dim \hom_G(E_n,E)$$

For all E_i not isomorphic to E, the summands are zero, and so we are left with d times the number of E_i isomorphic to E:

$$\dim \hom_G(V,E) = d \cdot \#\{E_i \text{ isomorphic to } E\}$$

And so we obtain that the number of E_i isomorphic to E is the aforementioned number. ■

1.4.5 Definition

Let V be a finite-dimensional G-representation, and E be an irreducible G-representation. Then the **multiplicity** of E in V, denoted $[V : E]$, is the number of irreducible components in a factorization of V isomorphic to V. That is,

$$[V : E] = \frac{\dim \hom_G(V, E)}{\dim \hom_G(E, E)}$$

Let V be a finite-dimensional G-representation, and E an irreducible one. Consider the G-subrepresentation of V obtained by taking the sum of all G-subrepresentations of V isomorphic to E. This is called the **isotypical component** V_E.

1.4.6 Lemma

Let $V = E_1 \oplus \cdots \oplus E_n$ be a factorization of V into a direct sum of irreducible G-subrepresentations. Then V_E is equal to the sum of the E_is isomorphic to E.

Proof

Clearly the sum of the E_is isomorphic to E is contained in V_E. Now, suppose that $F \subseteq V$ is isomorphic to E. We will show that given an E_i not isomorphic to E, composing the inclusion $F \to V$ with the projection $V \to E_i$ is 0. From this it follows that F must be contained in the sum of E_is isomorphic to E, giving us our desired result.

Indeed, since F is irreducible $F \to V \to E_i$ must be either zero or an isomorphism (by Schur). Since F is isomorphic to E which is not isomorphic to E_i, we get that this morphism must be zero, as desired. ■

Although the decomposition of V into a direct sum of irreducible subrepresentations is not necessarily unique, if we group the subrepresentations by isomorphism class, we get a result independent of the representation, the isotypical component of that isomorphism class.

Note that V_E has a unique complementary subrepresentation. Firstly it has one by Maschke. Let W be a complementary subrepresentation of V_E, then it decomposes into irreducible subrepresentations. That is, $W = F_1 \oplus \cdots \oplus F_n$, and so $V = V_E \oplus F_1 \oplus \cdots \oplus F_n$. In particular this means that if we group F_i by isomorphism class, we get $W = V_{F_1} \oplus \cdots \oplus V_{F_n}$, as required.

Let $\mathbb{F}$ be the trivial representation of G, i.e. $gx = x$ for all $x \in \mathbb{F}$. This is clearly irreducible, as it has dimension one. Notice that V^G is equal to the isotypical component $V_{\mathbb{F}}$. Let $E \subseteq V$ be isomorphic to $\mathbb{F}$, then since $\mathbb{F}$ is G-invariant so too must be E. And so $V_{\mathbb{F}} \subseteq V^G$. Let $E \subseteq V^G$ be irreducible, then it must be isomorphic to $\mathbb{F}$ (since every subvector-space of V^G is a subrepresentation, so the only irreducible subrepresentations are one-dimensional, and V^G's representation is trivial). Thus $V^G \subseteq V_{\mathbb{F}}$.

The kernel of the projection operator on V^G, Av_V^G, is thus the sum of all irreducible components of V not isomorphic to $\mathbb{F}$.

1.4.7 Lemma

Let $\mathbb{F}$ be algebraically closed, and E an irreducible G-representation. Then $\mathrm{end}_G(E) = \hom_G(E, E)$ is equal to $\mathbb{F} \cdot \mathrm{id}_E$.

Proof

Let $f : E \to E$ be an endomorphism of E. Since $\mathbb{F}$ is algebraically closed, f has an eigenvalue λ. Then $f - \lambda \mathrm{id}_E$ is also an endomorphism of E which is not invertible, and thus by Schur's lemma is zero. Therefore $f = \lambda \mathrm{id}_E$ as required. ■

Since $\hom_G(E,E)$ is one-dimensional for algebraically-closed $\mathbb{F}$ we have that

$$[V:E] = \frac{\dim \hom_G(V,E)}{\dim \hom_G(E,E)} = \dim \hom_G(V,E)$$

1.5 The regular representation

For a set X and a field $\mathbb{F}$, we define the vector space $\mathbb{F}[X]$ to be the space of all formal linear combinations of elements of X. For clarity, we will denote elements of X in $\mathbb{F}[X]$ by δ_x for $x \in X$. That is, $\mathbb{F}[X] = \{\sum_i a_i \delta_{x_i} \mid x_i \in X\}$. This is the free vector space over X.

1.5.1 Definition

The **regular G-set** is simply G, with the action given by left-multiplication by G: $\rho(g)(h) = gh$. The **regular G-representation** is $\mathbb{F}[G]$ with the action given by $\rho(g)(\delta_h) = \delta_{gh}$ (this defines a unique automorphism).

Recall that morphisms out of $\mathbb{F}[X]$ are determined uniquely by their image of X; $\hom(\mathbb{F}[X], V) \cong \mathrm{Set}(X, V)$. This is an isomorphism of vector spaces.

Let Set_G be the category of G-sets.

1.5.2 Lemma

Let X be a G-set and V a G-representation. Then the isomorphism of vector spaces $\hom(\mathbb{F}[X], V) \cong \mathrm{Set}(X, V)$ restricts to an isomorphism of vector spaces $\hom_G(\mathbb{F}[X], V) \cong \mathrm{Set}_G(X, V)$.

This is simple. Recall that $\hom_G(\mathbb{F}[X], V) \cong \hom(\mathbb{F}[X], V)^G$ has a trivial representation structure.

Let E be an irreducible G-representation, then

$$[\mathbb{F}[G]:E] = \frac{\dim \hom_G(\mathbb{F}[G], E)}{\dim \hom_G(E,E)} = \frac{\dim \mathrm{Set}_G(G,E)}{\dim \mathrm{end}_G(E)}$$

$\mathrm{Set}_G(G,E)$ is one-dimensional: for $f \in \mathrm{Set}_G(G,E)$ we have that $f(g) = gf(1)$ so $\mathrm{Set}_G(G,E) \cong E$ (by mapping f to $f(1)$). Thus

$$[\mathbb{F}[G]:E] = \frac{\dim E}{\dim \mathrm{end}_G(E)}$$

In particular, if $\mathbb{F}$ is algebraically closed then $\dim \mathrm{end}_G(E) = 1$ and so $[\mathbb{F}[G]:E] = \dim E$.

1.5.3 Corollary

There are finitely many isomorphism classes of irreducible G-representations.

Proof

By above, every irreducible G-representation occurs in $\mathbb{F}[G]$ $[\mathbb{F}[G]:E] > 0$ times. Since $\mathbb{F}[G]$ is finite-dimensional, it has finitely many non-isomorphic subspaces, and thus there can only be finitely many irreducible G-representations. ∎

Notice that in general, if $E_1, \ldots, E_n$ are all irreducible subrepresentations of V up to isomorphism. Now, $V = E_1^{\oplus [V:E_1]} \oplus \cdots \oplus E_n^{[V:E_n]}$ and so $\dim V = \sum_i [V:E_i] \dim E_i$. In particular if $E_1, \ldots, E_n$ list all irreducible G-representations up to isomorphism,

$$\dim \mathbb{F}[G] = \sum_i [\mathbb{F}[G]:E_i] \dim E_i$$

and if $\mathbb{F}$ is algebraically closed, $[\mathbb{F}[G]:E_i] = \dim E_i$, and so we get:

1.5.4 Corollary

Suppose that $\mathbb{F}$ is algebraically closed. Let $E_1, \ldots, E_n$ be all irreducible G-representations up to isomorphism. Then

$$|G| = \sum_i (\dim E_i)^2$$

1.5.5 Example

Consider the group $G = S_3$ (permutations on $\{0, 1, 2\}$). Let $\mathbb{F}$ be an algebraically closed field whose characteristic does not divide $|G| = 3!$, i.e. its characteristic is not 2 or 3. We have two irreducible one-dimensional representations of G: the trivial, and the other given by the sign character $\operatorname{sgn}: S_3 \to \{\pm 1\}$. We have already shown that the usual representation of S_3 on $\mathbb{F}^3$ has an irreducible subrepresentation of vectors whose entries sum to zero. This subrepresentation has dimension two, and we see that

$$|S_3| = 6 = 1 + 1 + 2^2$$

So these are all the irreducible S_3-representations, up to isomorphism

1.6 The group algebra

A ring here has an identity, but may be non-commutative.

1.6.1 Definition

A $\mathbb{F}$-algebra is a ring A which is also a $\mathbb{F}$-vector space, such that multiplication $A \times A \to A$ is bilinear.

Notice that if A is a $\mathbb{F}$-algebra, then we have a map $\mathbb{F} \to A$ given by $c \mapsto c \cdot 1$ (1 is the unit in A). This map is injective, so we can embed $\mathbb{F}$ in A. In fact, an equivalent formulation of a $\mathbb{F}$-algebra is a ring A together with a ring homomorphism $\mathbb{F} \to Z(A)$. Indeed, this map $(c \mapsto c \cdot 1)$ is a ring homomorphism $\mathbb{F} \to Z(A)$. And given a ring homomorphism $\sigma: \mathbb{F} \to Z(A)$, we can define $c \cdot a = \sigma(c)a$. This clearly defines a vector space over A, and multiplication is bilinear.

We recall the definition of an R-module, and R-module-morphisms.

Note that if A is a $\mathbb{F}$-algebra and M an A-module, then M can be naturally given the structure of a $\mathbb{F}$-vector space. This is since $\mathbb{F}$ embeds in A.

1.6.2 Definition

The **group algebra** of G, denoted $\mathbb{F}[G]$, is the vector space denoted as above with multiplication given by $\delta_g \delta_h = \delta_{gh}$.

Notice that if A is a $\mathbb{F}$-algebra, then there is a natural bijection

$$\operatorname{Alg}_{\mathbb{F}}(\mathbb{F}[G], A) \cong \operatorname{Grp}(G, A^\times)$$

(The left is morphisms of $\mathbb{F}$-algebras, and the right is morphisms of groups. $A^\times$ is the group of invertible elements of A.) This is given by sending $f: \mathbb{F}[G] \to A$ to the map $g \to f(\delta_g)$. This is well-defined since $f(\delta_g) f(\delta_{g^{-1}}) = f(\delta_1) = 1$ and so $f(\delta_g)$ are all invertible. This is also clearly a homomorphism: $f(\delta_{gh}) = f(\delta_g \delta_h) = f(\delta_g) f(\delta_h)$. Being a bijection and natural is also clear.

Note that $\mathbb{F}$-algebra homomorphisms $A \to \operatorname{end}(V)$ give rise to A-modules on V, and vice versa. Indeed: given $\sigma: A \to \operatorname{end}(V)$ define $a \cdot v = \sigma(a)(v)$.

1.6.3 Corollary

Let V be an $\mathbb{F}$-vector space, then there is a natural bijection between G-representations on V and $\mathbb{F}[G]$-modules on V.

Proof

G-representations on V are homomorphisms $G \to \mathrm{end}(V)^\times = \mathrm{GL}(V)$. $\mathbb{F}[G]$-modules on V are $\mathbb{F}$-algebra homomorphisms $\mathbb{F}[G] \to \mathrm{end}(V)$. Then apply the previous remark. ■

1.6.4 Proposition

Let V, W be two G-representations, so also $\mathbb{F}[G]$-modules. Then a linear morphism $T: V \to W$ is a morphism of G-representations if and only if it is a morphism of $\mathbb{F}[G]$-modules.

This is just definition chasing.

1.7 The non-commutative Fourier transform

As before, we assume that G is a finite group whose size is divisible in $\mathbb{F}$.

A division ring is one for which every nonzero element in the ring is invertible. A division algebra is an algebra which is a division ring as a ring.

1.7.1 Lemma (Schur)

Let E be an irreducible G-representation. Then $\mathrm{end}_G(E)$ is a division algebra.

This is immediate since every non-zero endomorphism is an isomorphism.

1.7.2 Lemma

Let A be a finite-dimensional division $\mathbb{F}$-algebra, then every subalgebra is also a division algebra.

Proof

Let B be a subalgebra of A, and let $b \in B$ be nonzero. Let $m \in \mathbb{F}[x]$ be the minimal polynomial of the linear map $\ell_b: A \to A$ given by left-multiplication by b. Note then that $m(\ell_b) = 0$ and so $m(\ell_b 1) = m(b) = 0$. We write $m(x) = xn(x) + c$, and we note that c must be nonzero as since ℓ_b is invertible (because b has an inverse), $\ell_b n(\ell_b) = 0$ would imply $n(\ell_b) = 0$, contradicting m's minimality. Since c is nonzero, it has an inverse in A. So $m(b) = 0$ means $bn(b) + c = 0$, so $bn(b) = -c$ and so $b^{-1} = -c^{-1}n(b)$. This is in B, as required. ■

1.7.3 Proposition

Suppose $\mathbb{F}$ is algebraically closed, and let A be a finite-dimensional division $\mathbb{F}$-algebra. Then $A = \mathbb{F}$.

Proof

Let $a \in A$, and take B be the subalgebra spanned by a: $B = \mathrm{span}\,\{a^n\}_{n\in\mathbb{N}}$. By the above lemma, B is itself

a division algebra. But B is commutative, and thus is a field, moreso a finite field extension of $\mathbb{F}$ (as it has finite dimension). But $\mathbb{F}$ is algebraically closed, so $B = \mathbb{F}$ (since all extensions of an algebraically closed field are transcendental). Thus $a \in \mathbb{F}$, so $A = \mathbb{F}$. ■

Note that we have stumbled upon another proof of Schur: $\operatorname{end}_G(E)$ is a division algebra, and since it is finite-dimensional, if $\mathbb{F}$ is algebraically closed it must be $\mathbb{F}$.

Note:
Modules over division rings behave similarly to modules over fields (vector spaces). For example, the proof that vector spaces have unique (up to size) bases is the same for modules over division rings. Moreso, linearly independent sets can be extended to bases.

If D is a $\mathbb{F}$-algebra, then we have that $\dim_{\mathbb{F}} V = \dim_D V \cdot \dim_{\mathbb{F}} D$ (the proof is similar as that for field extensions).

Let E be an irreducible G-representation, and let $D_E = \operatorname{end}_G(E)$ (it is a division algebra by Schur). Then we have a natural $\mathbb{F}$-algebra morphism

$$\mathcal{F}_E \colon \mathbb{F}[G] \to \operatorname{end}_{D_E}(E)$$

given by $\mathcal{F}_E(g)(x) = gx$. This is well-defined: $\mathcal{F}_E(g)$ is an endomorphism of E over D_E since $\mathcal{F}_E(g)(f \cdot e) = \mathcal{F}_E(g)(fe) = gfe$, and since f is a G-morphism, this is equal to $fge = f \cdot \mathcal{F}_E(g)(e)$.

Let $E_1, \dots, E_n$ list all the non-isomorphic irreducible representations of G. For each E_i we have $\mathcal{F}_{E_i} \colon \mathbb{F}[G] \to \operatorname{end}_{D_{E_i}}(E_i)$, and thus we can gather them into one large $\mathbb{F}$-algebra morphism

$$\mathcal{F} \colon \mathbb{F}[G] \to \prod_{i=1}^{n} \operatorname{end}_{D_{E_i}}(E_i)$$

This is called the **non-commutative Fourier transform** of G.

Let E and F be finitely-generated modules over a division $\mathbb{F}$-algebra D also of finite dimension. Then

$$\dim_{\mathbb{F}} \hom_D(E, F) = \dim_D E \cdot \dim_{\mathbb{F}} F = \frac{\dim_{\mathbb{F}} E \cdot \dim_{\mathbb{F}} F}{\dim_{\mathbb{F}} D}$$

Indeed, let $v_1, \dots, v_n$ be a basis of E over D, then $\hom_D(E, F)$ is isomorphic to F^r as $\mathbb{F}$-vector spaces: send T to $(Tv_1, \dots, Tv_n)$. The rest of the equality follows from towering dimensions.

1.7.4 Proposition (Artin-Wedderburn, special case)
$\mathcal{F}$ is an isomorphism of $\mathbb{F}$-algebras.

Proof

We show that $\mathcal{F}$ is an injection and that domain and codomain of $\mathcal{F}$ have equal dimension. To show that $\mathcal{F}$ is injective, suppose $\mathcal{F}(a) = 0$, so a acts trivially on each E_i. So a acts trivially on every finite-dimensional representation (as the sum of E_is), in particular it must act trivially on $\mathbb{F}[G]$. This is only possible if $a = 0$ (since $a = a \cdot 1 = 0$).

The dimension of the domain is $|G|$. Let $e_i = \dim_{\mathbb{F}} E_i$ and $d_i = \dim_{\mathbb{F}} D_{E_i}$. By above, we have that

$$\dim_{\mathbb{F}} \operatorname{end}_{D_{E_i}} E_i = \frac{(\dim_{\mathbb{F}} E_i)^2}{\dim_{\mathbb{F}} D_{E_i}} = e_i^2/d_i$$

And so we need to show that

$$|G| = \sum_{i=1}^{n} \frac{e_i^2}{d_i}$$

And indeed, recall that

$$|G| = \sum_{i=1}^{n} [\mathbb{F}[G] : E_i] \cdot \dim_{\mathbb{F}} E_i = \sum_{i=1}^{n} \frac{e_i^2}{d_i}$$

Since $[\mathbb{F}[G] : E_i] = e_i/d_i$ since we showed

$$[\mathbb{F}[G] : E] = \frac{\dim \hom_G(\mathbb{F}[G], E)}{\dim \operatorname{end}_G(E)} = \frac{\dim_{\mathbb{F}} E}{\dim_{\mathbb{F}} \operatorname{end}_G(E)}$$ ■

In the case that $\mathbb{F}$ is algebraically closed, we have that $D_{E_i} = \mathbb{F}$ and so $\mathcal{F}$ forms an isomorphism

$$\mathcal{F}\colon \mathbb{F}[G] \to \prod_{i=1}^{n} \operatorname{end}_{\mathbb{F}}(E_i)$$

So we can consider the group algebra to be the product of matrix alegbras.

1.7.5 Example

We can identify $\mathbb{F}[G]$ with $\operatorname{Set}(G, \mathbb{F})$ (map $f\colon G \to \mathbb{F}$ to $\sum_{g\in G} f(g)\delta_g$). Now notice that the center $Z(\mathbb{F}[G])$ are all functions $f\colon G \to \mathbb{F}$ for which for all $h\colon G \to \mathbb{F}$:

$$\left(\sum_{g\in G} f(g)\delta_g\right)\left(\sum_{g\in G} h(g)\delta_g\right) = \sum_{g\in G}\left(\sum_{ab=g} f(a)h(b)\right)\delta_g$$

is equal to

$$\sum_{g\in G}\left(\sum_{ab=g} h(a)f(b)\right)\delta_g$$

That is, $\sum_{ab=g} f(a)h(b) = \sum_{ab=g} f(b)h(a)$.
In particular, if we let h_x be the indicator of $x \in G$: $h_x(x) = 1$ and $h_x(y) = 0$, then we see that for $g \in G$,

$$\sum_{ab=g} f(a)h_x(b) = f(ax^{-1}) = f(x^{-1}a) = \sum_{ab=g} f(b)h_x(a)$$

So $f(gh) = f(hg)$ for all $g, h \in G$. Equivalently $f(hgh^{-1}) = f(g)$, i.e. f is a **class function**: it is identical on conjugacy classes.
This is also sufficient:

$$\sum_{ab=g} f(a)h(b) = \sum_{b\in G} f(gb^{-1})h(b) = \sum_{a\in G} f(a^{-1}g)h(a) = \sum_{ab=g} f(b)h(a)$$

So $Z(\mathbb{F}[G])$ can be identified with the set of class functions: $\operatorname{Set}(G, \mathbb{F})^{\mathsf{cl}}$.

1.7.6 Example

Let D be a division ring and V a finite-dimensional D-module. Then the morphism of rings $Z(D) \to Z(\operatorname{end}_D(V))$, which maps z to $v \mapsto zv$, is an isomorphism. Let $n = \dim V$, then $\operatorname{end}_D(V)$ is isomorphic to $\operatorname{Mat}_n(D^{\mathsf{op}})$ (D^{op} being the opposite ring of D). Indeed, let $B = \{v_1, \ldots, v_n\}$ form a basis for V, then mapping $T \in \operatorname{end}_D(v)$ to the representation matrix $[T]_B$ is an isomorphism. Note that this indeed must be in the opposite ring since

$$[T]_B[\sum_i d_i v_i]_B = \sum_i [Tv_i]_B \cdot^{\mathsf{op}} d_i = \sum_i d_i[Tv_i]_B = [T(\sum_i d_i v_i)]_B$$

A matrix in the center of $\operatorname{Mat}_n(D^{\mathsf{op}})$ must be a scalar matrix, whose entries are in $Z(D^{\mathsf{op}}) = Z(D)$. So the center of $Z(\operatorname{end}_D V)$ is isomorphic to $Z(D)$.

1.7.7 Corollary (Basic formula)

Let $\mathbb{F}$ be algebraically closed, then the cardinality of the set of isomorphism classes of irreducible G-representations is equal to the cardinality of the set of conjugacy classes of G.

Proof

By the above exercise, the center of $Z(\mathbb{F}[G])$ is isomorphic to $\mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$, the set of class functions. The dimension of the codomain of $\mathcal{F}$ is $\prod_{i=1}^{n} Z(\mathrm{end}_{D_{E_i}}(E_i))$, which by the above exercise is isomorphic to $\prod_{i=1}^{n} Z(D_{E_i})$. Since $\mathbb{F}$ is algebraically closed, $D_{E_i} \cong \mathbb{F}$, and so this is isomorphic to $\mathbb{F}^n$. Thus we have that $n = \dim \mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$, where n is the number of irreducible G-representations.

Let the conjugacy classes of G be $[g_1],\dots,[g_m]$. Define $f_i : G \to \mathbb{F}$ to be the indicator of $[g_i]$. This forms a basis of $\mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$ and as such $\dim \mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$ is equal to the number of conjugacy classes of G, thus completing our proof. ■

In total, let G be a finite group and $\mathbb{F}$ an algebraically closed field whose characteristic does not divide $|G|$. Let n be the number of conjugacy classes of G, and $d_1,\dots,d_n$ be the dimensions of the irreducible representations of G. Then

$$|G| = \sum_{i=1}^{n} d_i^2$$

1.7.8 Example

The following example will not be used, but is an example of a result of the above investigation. Define the **zeta function** of the group G to be

$$\zeta_G(s) = \sum_{i=1}^{n} d_i^{-s}$$

Note that $\zeta_G(0)$ is equal to the number of conjugacy classes in G, and $\zeta_G(-2)$ is equal to the number of elements in G. In general one has

$$\zeta_G(-2+2n) = \frac{1}{|G|^{2n-1}} \left| c_n^{-1}(1) \right|$$

where $c_n : G^{2n} \to G$ is given by $c_n(x_1,y_1,\dots,x_n,y_n) = [x_1,y_1]\cdots[x_n,y_n]$. (Note that $\left|c_n^{-1}(1)\right|$ is the cardinality of the fiber of 1.)

Let E be an irreducible G-representation. Then there is a unique element $e_E \in \mathbb{F}[G]$ which acts as the identity on irreducible subrepresentations isomorphic to E and as 0 on irreducible subrepresentations not isomorphic to E. Indeed, such an element must satisfy $\mathcal{F}(e_E) = (T_i)_i$ where $T_i = \mathrm{id}_{E_i}$ when $E_i \cong E$ and 0 otherwise. Due to $\mathcal{F}$'s bijectivity a unique element must exist.

Notice that $e_E \in Z(\mathbb{F}[G])$ and $e_E^2 = e_E$ (since $(T_i)_i$ satisfies this). And the action of e_E on any finite-dimensional G-representation V is the unique G-morphic projection onto the isotypic component V_E. So if we want a formula for this projection, we can equivalently find a formula for e_E: scalars c_g such that $e_E = \sum_g c_g \delta_g$. We shall return to this.

1.8 The commutative Fourier transform

In this section we will take G to be a finite Abelian group, and $\mathbb{F}$ to be algebraically closed where $|G| \in \mathbb{F}^\times$.

1.8.1 Proposition

All irreducible representations of G are one-dimensional.

Proof

Let $\rho: G \to \mathrm{GL}(E)$ be a representation. Then notice that $\rho(g): E \to E$ is a G-morphism: $\rho(g)(hv) = \rho(gh)(v) = \rho(hg)(v) = h\rho(g)v$ (we use both juxtaposition and ρ here to denote the same representation). So $\rho(g) \in \mathrm{end}(E)$, and by Schur (since $\mathbb{F}$ is algebraically closed), $\rho(g)$ is scalar multiplication. This means that any 1-dimensional space is a representation, and as such all irreducible representations must be 1-dimensional.

Define $\mathrm{ch}_{\mathbb{F}}(G)$ to be the set of characters of G, i.e. the set of group morphisms $G \to \mathbb{F}^\times$. Recall that every character $\chi \in \mathrm{ch}_{\mathbb{F}}(G)$ induces a one-dimensional representation (well, it simply *is* a representation since $\mathrm{GL}(\mathbb{F}) = \mathbb{F}^\times$, but I digress). We denote the representation induced by χ as $\mathbb{F}_\chi$.

1.8.2 Corollary

The family $(\mathbb{F}_\chi)_{\chi \in \mathrm{ch}_{\mathbb{F}}(G)}$ lists all the irreducible representations of G. (That is to say every irreducible representation of G is isomorphic to some $\mathbb{F}_\chi$, and every character induces a unique representation.)

Clearly $(\mathbb{F}_\chi)_\chi$ list all the one-dimensional (and thus irreducible) representations of G. And distinct characters induce non-isomorphic representations: if $f: \mathbb{F}_\chi \to \mathbb{F}_\mu$ is an isomorphism then $f(\chi(g)1) = \chi(g)f(1)$ by linearity, while $f(\chi(g)1) = \mu(g)f(1)$ by equivariance (G-morphism). Thus $\chi(g) = \mu(g)$.

Note that

$$|G| = \sum_{\chi \in \mathrm{ch}_{\mathbb{F}}(G)} (\dim \mathbb{F}_\chi)^2 = |\mathrm{ch}_{\mathbb{F}}(G)|$$

1.8.3 Example

If $\mathbb{F}$ is not algebraically closed, this is not true. For instance, let $G = \mu_3$ be the group of third roots of unity in $\mathbb{C}$: $\mu_3 = \{1, \omega_3, \omega_3^2\} = \langle \omega_3 \rangle$, and let $\mathbb{F} = \mathbb{R}$. Then $\mathbb{C}$ is a two-dimensional irreducible representation of μ_3 over $\mathbb{R}$, where μ_3 acts on $\mathbb{C}$ by multiplication.

Now note that the Fourier transform in the Abelian, algebraically-closed case reduces to

$$\mathcal{F}: \mathbb{F}[G] \to \prod_{\chi \in \mathrm{ch}_{\mathbb{F}}(G)} \mathrm{end}_{\mathbb{F}}(\mathbb{F}_\chi) = \prod_{\chi \in \mathrm{ch}_{\mathbb{F}}(G)} \mathbb{F} = \mathrm{Set}(\mathrm{ch}_{\mathbb{F}}(G), \mathbb{F})$$

The algebra structure of the right side is given by pointwise multiplication. Originally, $\mathcal{F}$ sent δ_g to the action of multiplication by g on each $\mathbb{F}_\chi$. Which means that $\mathcal{F}$ sent δ_g to $c \mapsto \chi(g)c$. In the Abelian case, this means that $\mathcal{F}$ sends δ_g to the function $\mathcal{F}(g): \mathrm{ch}_{\mathbb{F}}(G) \to \mathbb{F}$ which maps χ to $\chi(g)$. So

$$\mathcal{F}\left(\sum_{g \in G} c_g g\right)(\chi) = \sum_{g \in G} c_g \chi(g)$$

Naturally, we can ask ourselves to find an inverse for $\mathcal{F}$. Since $\mathrm{Set}(\mathrm{ch}_{\mathbb{F}}(G), \mathbb{F})$ is generated by $\{\delta_\chi\}_{\chi \in \mathrm{ch}_{\mathbb{F}}(G)}$, where $\delta_\chi(\chi) = 1$ and $\delta_\chi(\mu) = 0$ for $\chi \neq \mu$, it is sufficient to find the inverse image of δ_χ. So we want to find $e_\chi = \sum_{g \in G} c_g \delta_g$ such that $\mathcal{F}(e_\chi) = \delta_\chi$. That is,

$$\mathcal{F}\left(\sum_{g \in G} c_g \delta_g\right) = \delta_\chi$$

So for $\mu \in \mathrm{ch}_{\mathbb{F}}(G)$, we need

$$\mathcal{F}(e_\chi)(\mu) = \sum_{g \in G} c_g \mu(g) = \delta_\chi(\mu)$$

In particular, we need $\sum_{g \in G} c_g \chi(g) = 1$. So an initial guess (and the correct one) will be $c_g = \chi(g)^{-1}/|G|$, i.e. $e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g)^{-1} \delta_g$.

And we see for $\mu \neq \chi$:

$$\mathcal{F}(e_\chi)(\mu) = \frac{1}{|G|}\sum_{g\in G}\chi(g)^{-1}\mu(g) = \frac{1}{|G|}\sum_{g\in G}(\mu\chi^{-1})(g)$$

Setting $\theta = \mu\chi^{-1}$, since $\mu \neq \chi$ there is some $g_0 \in G$ such that $\theta(g_0) \neq 1$. Then

$$\sum_{g\in G}\theta(g) = \sum_{g\in G}\theta(g_0 g) = \theta(g_0)\sum_{g\in G}\theta(g)$$

Solving for this gives $\sum_{g\in G}\theta(g) = 0$, as required.

Now notice that

$$\mathcal{F}(\delta_g) = (\chi(g))_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)} = \sum_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)}\chi(g)\delta_\chi$$

Applying the inverse Fourier transform, we get

$$\delta_g = \sum_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)}\chi(g)e_\chi$$

Now, $\{e_\chi\}_\chi$ forms a basis for $\mathbb{F}[G]$ (since $\mathcal{F}(e_\chi) = \delta_\chi$ forms a basis for $\mathrm{Set}(\mathrm{ch}_{\mathbb{F}}(G), \mathbb{F})$). This gives us two bases for $\mathbb{F}[G]$:

(1) The *geometric basis* $\{\delta_g\}_{g\in G}$, and

(2) The *spectral basis* $\{e_\chi\}_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)}$.

The change-of-basis matrices are

$$e_\chi = \sum_{g\in G}\frac{1}{|G|}\chi(g)^{-1}\delta_g$$
$$\delta_g = \sum_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)}\chi(g)e_\chi$$

Notice that characters are elements of $\mathbb{F}[G]$: $\chi = \sum_{g\in G}\chi(g)\delta_g$. Quickly, this gives us $\chi = |G|e_{\chi^{-1}}$ (where χ^{-1} is the multiplicative inverse of χ). So

$$\delta_g = \sum_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)}\chi(g)e_\chi = \frac{1}{|G|}\sum_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)}\chi(g)e_{\chi^{-1}} = \frac{1}{|G|}\sum_{\chi\in \mathrm{ch}_{\mathbb{F}}(G)}\chi(g)^{-1}e_\chi$$

We now provide an application of the Fourier transform for finite Abelian groups:

1.8.4 Theorem (Dirichlet)

Let $d \in \mathbb{Z}_{\geq 1}$ and $a \in \mathbb{Z}$ be relatively prime. Then there exist infinitely many primes p such that $p \equiv a \pmod{d}$.

Proof

Consider the group $(\mathbb{Z}/d\mathbb{Z})^\times$ (the Euler group of numbers invertible modulo d). Given a function $f \in \mathrm{Set}((\mathbb{Z}/d\mathbb{Z})^\times, \mathbb{C})$, we can extend it to a function on all of $\mathbb{Z}/d\mathbb{Z}$ by setting it to be 0 on non-invertible elements. Then consider

$$M_f(s) = \sum_{p \text{ prime}}\frac{f([p]_d)}{p^s}$$

where $[\bullet]_d\colon \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ is the canonical projection. We assume that $s \in \mathbb{R}$. Note that when $s > 1$, the series $M_f(s)$ is bound by $\sum_n n^{-s}$ and therefore converges.

Let $\delta_a\colon (\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}$ be the Kronecker delta for $[a]_d$ (i.e. $\delta_a([a]_d) = 1$ and 0 everywhere else), then notice

that

$$M_f(s) = \sum_{p \text{ prime}} \frac{\delta_a([p]_d)}{p^s}$$

Now if M_f is unbounded from 1 on the right, then there must be infinitely many non-zero terms in the series, meaning infinitely many primes where $\delta_a([p]_d) = 1$, i.e. $p \equiv a \pmod{d}$.
We will prove this with help from the following proposition.

1.8.5 Proposition

Let $\chi \in \mathrm{ch}_{\mathbb{C}}((\mathbb{Z}/d\mathbb{Z})^\times)$ be a character not equal to 1. Then $|M_\chi(s)|$ is bounded as s tends to 1 from the right. If $\chi = 1$, then $M_\chi(s)$ is unbounded as s tends to 1 from the right.

If we prove this proposition, then we have proven our theorem. Recall that using $\mathrm{ch}_{\mathbb{C}}((\mathbb{Z}/d\mathbb{Z})^\times)$ as a basis for our group algebra, we have as before

$$\delta_a = \frac{1}{|(\mathbb{Z}/d\mathbb{Z})^\times|} \sum_{\chi \in \mathrm{ch}_{\mathbb{C}}((\mathbb{Z}/d\mathbb{Z})^\times)} \chi(a)^{-1}\chi$$

Thus in this sum, the trivial character 1 appears with non-zero coefficient. Now,

$$M_{\delta_a} = \frac{1}{|(\mathbb{Z}/d\mathbb{Z})^\times|} \sum_{\chi \in \mathrm{ch}_{\mathbb{C}}((\mathbb{Z}/d\mathbb{Z})^\times)} \chi(a)^{-1}M_\chi$$

so M_{δ_a} is the sum of finitely many bounded functions (M_χ for $\chi \neq 1$), and one unbounded function (M_1). Thus M_{δ_a} is unbounded, as required.

Proof

For $x \in \{z \in \mathbb{C} \mid |z| < 1\}$, we have that $-\log(1-x) = \sum_m x^m/m$. Now let us assume that $|f| \leq 1$, and let us define $a_p(s) = \frac{f([p]_d)}{p^s}$, so that $M_f(s) = \sum_p a_p(s)$. Let us consider

$$\sum_{p \text{ prime}} |-\log(1-a_p(s)) - a_p(s)| = \sum_{p \text{ prime}} \left|\sum_{m=2}^{\infty} \frac{a_p(s)^m}{m}\right| \leq \sum_p \sum_m \frac{1}{mp^{sm}}$$

We consider $s > 1$, and as such

$$\leq \sum_p \sum_m \frac{1}{p^m} = \sum_p \frac{1}{p^2}\frac{1}{1-1/p} \leq 2\sum_p \frac{1}{p^2} \leq 2\sum_n \frac{1}{n^2}$$

So we can deduce that if $|f| \leq 1$, then $M_f(s)$ is (un)bounded as s tends to 1 from the right iff

$$\ell_f(s) = \sum_{p \text{ prime}} -\log\left(1 - \frac{f([p]_d)}{p^s}\right)$$

is (un)bounded. Exponentiating, we can equivalently see if

$$L_f(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{f([p]_d)}{p^s}}$$

is bounded (or unbounded or zero).
Notice that for a finite N, let X_N be the set of integers whose prime factors are $\leq N$. Then notice that

$$\prod_{p \leq N} \frac{1}{1 - \chi([p]_d)p^{-s}} = \sum_{n \in X_N} \frac{\chi([n]_d)}{n^s}$$

We prove this by induction.

For brevity, let us define

$$L_f(s, N) = \prod_{p \leq N} \frac{1}{1 - f([p]_d)p^{-s}}$$

So we claim that

$$L_\chi(s, N) = \sum_{n \in X_N} \frac{\chi([n]_d)}{n^s}$$

For the case $N = 1$, we have that $X_N = \{1\}$ and the product is empty (1). We will write $\chi(\bullet)$ for $\chi([\bullet]_d)$ for brevity; we get $1 = \chi(1)$ which is indeed true (since χ is a character). Now notice that for $N + 1$ not prime, $X_{N+1} = X_N$ and the product is the same as well. So the only interesting case is when $N = P - 1$, in which case $X_P = \bigcup_{k=0}^{\infty} P^k X_{P-1}$. We get

$$\sum_{n \in X_P} \frac{\chi(n)}{n^s} = \sum_{k=0}^{\infty} \sum_{n \in X_{P-1}} \frac{\chi(P^k n)}{(P^k n)^s}$$

by χ's multiplicity, this is equal to

$$\sum_{k=0}^{\infty} \frac{\chi(P)^k}{P^{sk}} \sum_{n \in X_{P-1}} \frac{\chi(n)}{n^s} = \sum_{k=0}^{\infty} \frac{\chi(P)^k}{P^{sk}} L_\chi(s, P-1)$$

This is a geometric series, whose sum is

$$L_\chi(s, P-1) \cdot \frac{1}{1 - \chi(P)P^{-s}} = \prod_{p \leq P-1} \frac{1}{1 - \chi(p)p^{-s}} \cdot \frac{1}{1 - \chi(P)P^{-s}} = L_\chi(s, P)$$

as required.

As $N \to \infty$, we notice that $X_N \to \mathbb{Z}_{\geq 1}$ and the set of primes $\leq N$ is all of the primes, so we have our desired result.

Note that this hinges on $|\chi(n)| \leq 1$. This is true since n (for $n \in (\mathbb{Z}/d\mathbb{Z})^\times$) has finite order, so $\chi(n)$ must too. The only elements of $\mathbb{C}^\times$ with finite order are the roots of unity, so $|\chi(n)| = 1$.

So we have shown

$$L_\chi(s) = \sum_{n=1}^{\infty} \frac{\chi([n]_d)}{n^s}$$

Now notice that $L_1(s) = \sum_n \frac{1}{n^s}$. This clearly tends to $+\infty$ as $s \to 1^+$, so we have our result for $\chi = 1$.

For $\chi \neq 1$, we note that $L_\chi(s) \to L_\chi(1)$ for $s \to 1^+$. $L_\chi(1) \neq 0$ (this is a technical point, we will not show it here). And thus we have completed the proof (modulo some technicalities arising from analysis). ■

1.9 The classical Fourier transform

Viewing $\mathbb{F}[G]$ as the function space $\mathrm{Set}(G, \mathbb{F})$, we can view the Fourier transform as

$$\mathcal{F}\colon \mathrm{Set}(G, \mathbb{F}) \to \prod_i \mathrm{end}_{D_{E_i}}(E_i)$$

Recall that the algebra $\mathrm{Set}(G, \mathbb{F})$ has multiplication given by convolution: writing $f = \sum_{g \in G} f(g)\delta_g$ we have

$$f_1 * f_2 = \sum_{g \in G} f_1(g)\delta_g \sum_{h \in G} f_2(h)\delta_h = \sum_{g,h \in G} f_1(g)f_2(h)\delta_{gh} = \sum_{g \in G} \left(\sum_{h \in G} f_1(h)f_2(h^{-1}g) \right) \delta_g$$

i.e. $(f_1 * f_2)(g) = \sum_{h \in G} f_1(h)f_2(h^{-1}g)$ which is precisely the definition of a convolution.

On the other hand, the product space (the codomain of $\mathcal{F}$) has its multiplication defined by (pointwise) function composition. That is, $\mathcal{F}(f_1 * f_2) = \mathcal{F}(f_1) \circ \mathcal{F}(f_2)$.

In the case of Abelian G, the Fourier transform becomes

$$\mathcal{F}\colon \mathrm{Set}(G, \mathbb{F}) \to \mathrm{Set}(\mathrm{ch}_{\mathbb{F}}(G), \mathbb{F})$$

And function composition in the codomain becomes pointwise *multiplication*. This is because the functions in the product space are scalar multiplications, and composition is equivalent to multiplication. So we can write $\mathcal{F}(f_1 * f_2) = \mathcal{F}(f_1) \cdot \mathcal{F}(f_2)$, which is reminiscent of the classical Fourier transform.

Recall that the classical discrete Fourier transform takes a sequence of complex numbers $x_0, \ldots, x_{N-1}$ and transforms them into a new sequence of complex numbers $X_0, \ldots, X_{N-1}$ defined by

$$X_k = \sum_{n=0}^{N-1} x_n \omega_N^{-kn}$$

where ω_N is the primitive root of unity $\exp(2\pi i/N)$.

Now, we can view series of complex numbers as functions $(x_i)_i \colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$. So we can ask ourselves, what if we take the Abelian Fourier transform of this function? We see that $(x_i)_i = \sum_{i=0}^{N-1} x_i \delta_i$, and so

$$\mathcal{F}((x_i)_i) = \sum_{n=0}^{N-1} x_n \sum_{\chi \in \mathrm{ch}_{\mathbb{C}}(\mathbb{Z}/N\mathbb{Z})} \chi(n) \delta_\chi$$

Now, we ask ourselves, what are the characters of $\mathbb{Z}/N\mathbb{Z}$ over $\mathbb{C}$? Since $\mathbb{Z}/N\mathbb{Z}$ is cyclic, every group morphism $\mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times$ is determined by its image on 1. And since 1 has order N in $\mathbb{Z}/N\mathbb{Z}$, $\chi(1)^N = 1$ in $\mathbb{C}$, so $\chi(1)$ is an Nth root of unity, that is $\chi(1) = \omega_N^k$ for some $0 \leq k < N$. We claim that $\chi \mapsto \chi(1)$ gives a bijection between characters and $\mu_N(\mathbb{C})$ (Nth roots of unity). It is simple to see that every ω_N^k gives rise to a character. Furthermore, $\mu_N(\mathbb{C}) \cong \mathbb{Z}/N\mathbb{Z}$ (generated by ω_N), so we can view the Fourier transform as a function

$$\mathcal{F} \colon \mathrm{Set}(\mathbb{Z}/N\mathbb{Z}, \mathbb{C}) \to \mathrm{Set}(\mathbb{Z}/N\mathbb{Z}, \mathbb{C})$$

Now we return to our computation. We take the bijection between $\mathbb{Z}/N\mathbb{Z}$ and $\mathrm{ch}_{\mathbb{C}}(\mathbb{Z}/N\mathbb{Z})$ which maps $[n]$ to $\chi_n(1) = \omega_N^{-n}$. Note that the exact bijection we choose will not affect the outcome; it only affects the order of the resulting series. Since χ_n is a character, $\chi_n(k) = \chi_n(1)^k = \omega_N^{-kn}$. Thus we get

$$\mathcal{F}((x_i)_i) = \sum_{n=0}^{N-1} x_n \sum_{k=0}^{N-1} \omega_N^{-kn} \delta_k = \sum_{k=0}^{N-1} \left(\sum_{n=0}^{N-1} x_n \omega_N^{-kn} \right) \delta_k$$

i.e. $\mathcal{F}((x_i)_i)$ is the series $(X_k)_k$ defined by

$$X_k = \sum_{n=0}^{N-1} x_n \omega_N^{-kn}$$

which is precisely the discrete Fourier transform.

Now, we want to find the inverse discrete Fourier transform, namely x_n in terms of X_k. To do this we find the inverse of δ_{χ_k} (where $\chi_k(1) = \omega_N^{-k}$). This is $e_k = e_{\chi_k}$:

$$e_k = \frac{1}{N} \sum_{n=0}^{N-1} \chi_k(n)^{-1} \delta_n = \frac{1}{N} \sum_{n=0}^{N-1} \omega_N^{nk} \delta_n$$

Now, $(X_k)_k = \sum_{k=0}^{N-1} X_k \delta_{\chi_k}$, and so the inverse discrete Fourier transform of that is

$$(x_n)_n = \sum_{k=0}^{N-1} X_k e_k = \frac{1}{N} \sum_{k=0}^{N-1} X_k \sum_{n=0}^{N-1} \omega_N^{nk} \delta_n$$

Moving things around, we get

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k \omega_N^{nk}$$

2 Rings and Modules

2.1 Finiteness properties of modules and rings

2.1.1 Definition

Let M be an R-module. It is **Noetherian** (resp. **Artinian**) if it has no infinite strictly increasing (resp. decreasing) sequence of R-submodules.

2.1.2 Example

If R is a $\mathbb{F}$-algebra for some field $\mathbb{F}$, then every R-module can be regarded as a $\mathbb{F}$-vector space. In particular, if M is finite-dimensional as a $\mathbb{F}$-vector space, then it is both Noetherian and Artinian. Indeed, submodules are subspaces, and a chain of subspaces must have distinct dimensions.

2.1.3 Theorem

An R-module M is Noetherian if and only if every submodule of M is finitely generated.

Proof

Suppose that M is Noetherian, and let $N \subseteq M$ be a submodule. Assume that N is not finitely generated, then for every finite set of elements $v_1, \dots, v_n \in N$, $Rv_1 + \cdots + Rv_n \neq N$. We will construct an infinite increasing sequence of finitely generated submodules of N. Define $N_0 = 0$, and if $N_n = Rv_1 + \cdots + Rv_n$, since this cannot be equal to N there is a $v_{n+1} \in N - N_n$. Define $N_{n+1} = N_n + Rv_{n+1}$. This is an infinite sequence of strictly increasing submodules.

Now conversely suppose that every submodule of M is finitely generated. Let $M_1 \subseteq M_2 \subseteq \cdots$ be an increasing sequence of submodules in M. Let $N = \bigcup_n M_i$ be their union, which is itself a submodule of M. By assumption N is finitely generated, $N = Rv_1 + \cdots + Rv_n$. Since the M_i form a chain, we must have that all $v_i \in M_N$ for some N. But then $N = M_N$, so the chain is finite. ■

2.1.4 Lemma

Let M be an R-module and $N \subseteq M$ a submodule. Then M is Noetherian (resp. Artinian) iff N and M/N are.

Proof

We prove only the case for Noetherian modules, the Artinian case is handled similarly. If M is Noetherian, then clearly every submodule is too (since submodules of N are submodules of M). And submodules of M/N are of the form L/N for $N \subseteq L \subseteq M$, so a chain of M/N submodules is of the form

$$L_1/N \subseteq L_2/N \subseteq \cdots$$

and so $L_1 \subseteq L_2 \subseteq \cdots$ forms a chain of M submodules, and thus must be finite as well.

Conversely, if N and M/N are Noetherian then let $M_1 \subseteq M_2 \subseteq \cdots$ be a chain of M submodules. Consider then $M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots$, a chain of N submodules. Since N is Noetherian this must be finite, i.e. $M_i \cap N = M_k \cap N$ for $i \geq k$ for some k. Similarly consider $(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \cdots$, a chain of M/N submodules. Once again this must be finite, so $(M_i + N)/N = (M_k + N)/N$ for some $i \geq k$ (we can assume wlog that this is the same k). This means $M_i + N = M_k + N$ and $M_i \cap N = M_k \cap N$, which means that if $x \in M_i$ then

$$x \in (M_i + N) \cap M_i = (M_k + N) \cap M_i = M_k \cap M_i + N \cap M_i = M_k \cap M_i + N \cap M_k \subseteq M_k$$

So $M_i = M_k$, as required. ■

2.1.5 Corollary

The direct sum of finitely many Noetherian (resp. Artinian) modules is Noetherian (resp. Artinian).

Proof

Indeed, suppose M, N are Noetherian (or Artinian). Then $M \oplus 0 \subseteq M \oplus N$ is Noetherian, and $(M \oplus N)/(M \oplus 0) \cong N$ is also Noetherian. By our above lemma, this means $M \oplus N$ is Noetherian. ■

Recall that R is itself a left R-module, and submodules correspond to left ideals. R is then Noetherian if it has no infinite strictly increasing sequence of left ideals, and it is Artinian if it has no infinite decreasing sequence of left ideals. There is of course the dual notion of a right Noetherian (Artinian) ring, where we consider right ideals.

2.1.6 Example

R is left Noetherian (Artinian) if and only if all finitely generated R-modules are Noetherian (Artinian).

Indeed, if R is left Noetherian and M is finitely generated, then suppose $M = Rv_1 + \cdots + Rv_n$. Then let $f: R^n \to M$ be the R-module morphism defined by $f(r_1, \ldots, r_n) = r_1v_1 + \cdots + r_nv_n$. This is surjective, and as such $M \cong R^n/\ker f$. Since R^n is the direct sum of finitely many copies of R, it is Noetherian. As such, all quotients of it are Noetherian, M included.

And conversely if all finitely generated R-modules are Noetherian, then R is too (as a finitely generated R-module).

2.1.7 Definition

An R-module M is **simple** (or **irreducible**) if M is nonzero and has no non-trivial proper submodules (i.e. all submodules of M are either M or zero).

2.1.8 Proposition

If $I \subseteq R$ is a maximal left ideal, then R/I is a simple R-module. And all simple R-modules are isomorphic to some quotient of this form.

In other words, if we define $\mathfrak{M}_R$ to be the set of maximal left ideals of R, and $\mathfrak{S}_R$ to be the set of isomorphism classes of simple R-modules, we obtain a surjection

$$\mathfrak{M}_R \to \mathfrak{S}_r, \qquad I \mapsto R/I$$

Proof

R/I being simple is, simple. A submodule of R/I is a quotient of the form J/I where $I \subseteq J \subseteq R$ is a left ideal. Since I is maximal, this means that J/I must be trivial.

Let M be a simple R-module, and define $f: R \to M$ by $f(r) = ra$ for some nonzero $a \in M$. Now, $\operatorname{im} f$ is a nonzero submodule in M, and as such it must be all of M. By the isomorphism theorem, this means $R/\ker f \cong M$. Now $\ker f$ must be maximal: if $\ker f \subseteq I$ then $R/I \subseteq R/\ker f$ (by the injection $r+I \mapsto r+\ker f$, which is injective since if $r \in \ker f$ then $r \in I$). Since M is simple, then R/I is either 0 (so $I = R$) or M (so $I = \ker f$), thus $\ker f$ is maximal. ■

2.1.9 Theorem (Schur)

A morphism between simple R-modules is either zero or an isomorphism.

2.1.10 Definition

An R-module M is **semisimple** if every submodule $N \subseteq M$ has a complementary submodule $L \subseteq M$ such that $M = N \oplus L$.

2.1.11 Lemma

(1) The direct sum of finitely many semisimple modules is semisimple.

(2) A submodule of a semisimple module is semisimple.

(3) A quotient of a semisimple module is semisimple.

Proof

(1) Let M_1, M_2 be semisimple and let $N \subseteq M_1 \oplus M_2$. Let $p_1 \colon M_1 \oplus M_2 \to M_1$ be the projection operator, and view $M_2 \subseteq M_1 \oplus M_2$ by inclusion. Since M_1, M_2 are semisimple there exist $N_i \subseteq M_i$ such that

$$M_1 = p_1(N) \oplus N_1, \qquad M_2 = (N \cap M_2) \oplus N_2$$

Now we claim that $M_1 \oplus M_2 = N \oplus (N_1 \oplus N_2)$.

Clearly their intersection is zero: $n \in N \cap (N_1 \oplus N_2)$ means that $p_1(n) \in p_1(N) \cap N_1 = 0$. So $p_1(n) = 0$. Thus $n \in M_2$ and so $n \in N \cap M_2 \cap N_2 = 0$, so $n = 0$.

Let $m = (m_1, m_2) \in M_1 \oplus M_2$, then $m_1 = p_1(m) = p_1(n) + n_1$ for $n \in N$ and $n_1 \in N_1$. Then $p_1(m - (n + n_1)) = 0$ so $m - (n + n_1) \in M_2$. This means there exists $n' \in M_2 \cap N$ and $n_2 \in N_2$ such that $m - (n + n_1) = n' + n_2$ and so $m = (n + n') + n_1 + n_2 \in N \oplus (N_1 \oplus N_2)$.

(2) Let $N \subseteq M$ be a submodule, we want to show it too is semisimple. Let $L \subseteq N$ be a submodule, then there exists $L' \subseteq M$ such that $M = L \oplus L'$. But then $N = L \oplus (L' \cap N)$.

(3) Let $N \subseteq M$ be a submodule, we want to show that M/N is semisimple. Let $L \subseteq M/N$ then there exists an $L' \subseteq M$ such that $M = L' \oplus p^{-1}(L)$ where $p \colon M \to M/N$ is the canonical projection. Now $M/N = p(L') \oplus L$: for $m \in M$, $m = \ell' + \ell$, then $p(m) = p(\ell') + p(\ell) \in p(L') + L$. Note that $pp^{-1} = \mathrm{id}$ since p is surjective, and so $p(L') \cap L = p(L' \cap p^{-1}L) = p(0) = N$. ■

2.1.12 Proposition

Let M be a finitely generated R-module, then it is semisimple if and only if it can be written as a finite direct sum of simple modules.

Proof

If M can be written as a finite direct sum of simple modules, then since simple modules are semisimple, it too is semisimple.

Conversely suppose M is semisimple, and let $N \subseteq M$. Then N has a complement: $M = N \oplus N'$. The

projection operator $M \to N$ is surjective with kernel N', so $M/N' \cong N$. This shows us that N must be finitely generated: M is, so M/N' is. Thus M is Noetherian, as all its submodules are finitely generated.

We now claim that every nonzero submodule of M contains a maximal proper submodule. Indeed, let $N \subseteq M$ be a nonzero submodule. Suppose that N has no maximal proper submodule: then by choosing an initial proper submodule we can create an increasing chain of submodules of N: $N_1 \subseteq N_2 \subseteq \cdots$, a contradiction since N is Noetherian as a submodule of M.

If M is zero, the claim is trivial, so suppose $M \neq 0$. Otherwise, let $N_1 \subseteq M$ be a maximal proper submodule and let $E_1 \subseteq M$ be a complement. Since N_1 is maximal, E_1 must be simple. If N_1 is zero, we are done. Otherwise we take $N_2 \subseteq N_1$ maximal and E_2 its simple complement, and continue. Thus we have simple $E_1, E_2, \ldots$ with an increasing sequence

$$E_1, E_1 \oplus E_2, \ldots$$

Since M is Noetherian, this must be finite. But then $M = E_1 \oplus \cdots \oplus E_n$. ■

2.1.13 Proposition

Let R be left Artinian. Then the set of isomorphism classes of simple R-modules is finite.

Proof

Suppose $E_1, E_2, \ldots$ is an infinite sequence of non-isomorphic simple R-modules. Choose nonzero $e_i \in E_i$, and let I_i be the annihilator of e_i:

$$I_i = \{x \in R \mid xe_i = 0\}$$

This is a left ideal of R, and we have an isomorphism $R/I_i \cong E_i$ (indeed, $r \mapsto re_i$ has kernel I_i).

We claim that I_{n+1} does not contain $I_1 \cap \cdots \cap I_n$. If we can demonstrate this, then $\bigcap_{i=1}^{n} I_i$ forms an infinite descending chain, contradicting R being left Artinian.

Now, suppose that $I_1 \cap \cdots \cap I_n \subseteq I_{n+1}$. Notice that the module morphism $R \to E_1 \oplus \cdots \oplus E_n$ given by $x \mapsto (xe_1, \ldots, xe_n)$ has kernel $I_1 \cap \cdots \cap I_n$. Thus it induces an injective morphism $R/(I_1 \cap \cdots \cap I_n) \to E_1 \oplus \cdots \oplus E_n$. Since $E_1 \oplus \cdots \oplus E_n$ is semisimple as a direct sum of semisimple modules, and so $R/(I_1 \cap \cdots \cap I_n)$ has a complementary submodule, and thus the projection operator provides a surjection $E_1 \oplus \cdots \oplus E_n \to R/(I_1 \cap \cdots \cap I_n)$. Since $I_1 \cap \cdots \cap I_n \subseteq I_{n+1}$, there is a surjection $R/(I_1 \cap \cdots \cap I_n) \to R/I_{n+1} \cong E_{n+1}$. And all in all, we have a surjection $E_1 \oplus \cdots \oplus E_n \to E_{n+1}$.

In particular this is a non-zero map, and as such one of the factor $E_i \to E_{n+1}$ must be nonzero. By Schur this means that $E_i \cong E_{n+1}$, a contradiction. ■

2.1.14 Corollary

If G is a finite group, then the set of isomorphism classes of irreducible G-representations over $\mathbb{F}$ is finite.

Note that we have dropped the condition that $|G| \in \mathbb{F}^\times$.

Proof

This follows immediately, since irreducible G-representations are simple $\mathbb{F}[G]$-submodules, and $\mathbb{F}[G]$, as a finite-dimensional algebra over a field, is Artinian. ■

2.2 Semisimple rings

2.2.1 Definition

A ring R is **(left) semisimple** if it is semisimple as an R-module.

2.2.2 Lemma

R is semisimple iff all finitely generated R-modules are semisimple.

Proof

Since R is a finitely generated R-module, one direction is trivial. Now suppose that R is semisimple, and let M be a finitely generated R-module. Then there exists a surjection $R^n \to M$, and as such M is isomorphic to a quotient of R^n. R^n is semisimple as the direct sum of semisimple modules, and quotients of semisimple modules are semisimple. ■

2.2.3 Example

Let G be a group and $\mathbb{F}$ a field with $|G| \in \mathbb{F}^\times$. Then Maschke's theorem says all $\mathbb{F}[G]$-modules which are finite-dimensional $\mathbb{F}$-vector spaces are semisimple. In particular, $\mathbb{F}[G]$ is a finite-dimensional $\mathbb{F}$-vector space, and as such $\mathbb{F}[G]$ is a semisimple $\mathbb{F}$-algebra.

2.2.4 Example

Division rings are simple, and thus semisimple. Indeed, D has no nontrivial submodules: for $0 \neq e \in D$, $De = D$.

2.2.5 Example

Let D be a division ring and V a finite-dimensional D-module. Then $\mathrm{end}_D(V)$ is a semisimple ring. Indeed, let $e_1, \ldots, e_n$ form a basis for V. Then let $L_i \subseteq \mathrm{end}_D(V)$ be the submodule of operators which are zero on e_j for $j \neq i$. Then L_i is a left ideal in $\mathrm{end}_D(V)$, and clearly $\mathrm{end}_D(V) = L_1 \oplus \cdots \oplus L_n$.

Finally, each L_i is simple. Indeed, given $T_1, T_2 \in L_i$ there is an $S \in \mathrm{end}_D(V)$ such that $S(T_1(e_i)) = T_2(e_2)$ (like in linear algebra). Then $ST_1 = T_2$ (since $ST_1(e_j) = 0$ for $i \neq j$), and as such L_i is simple.

Further note, with the D^{op}-module $V = (D^{\mathrm{op}})^n$, we have $\mathrm{end}_{D^{\mathrm{op}}}(V) \cong M_n(D)$. So we could restate this by saying that $M_n(D)$ are semisimple for D a division ring.

2.2.6 Proposition

A semisimple ring is both Noetherian and Artinian.

Proof

Since R is semisimple and a finitely-generated R-module, it can be written as a finite direct sum of simple R-modules. Simple R-modules are clearly Noetherian and Artinian, and their finite direct sums are as well. ■

2.2.7 Corollary

The set of isomorphism classes of simple R-modules, for a semisimple R, is finite.

Proof

R is Artinian, and the claim follows. ■

2.3 The Artin-Wedderburn Theorem

If M is an R-module, let $S = \mathrm{end}_R(M)$. Then M can be viewed as an S-module: for $T \in S$ and $m \in M$, $T \cdot m = Tm$.

2.3.1 Proposition (Jacobson's Density Theorem)

Let M be a semisimple R-module, and let $S = \mathrm{end}_R(M)$. Given $T \in \mathrm{end}_S(M)$ and $v_1, \ldots, v_n \in M$ then there exists an $r \in R$ such that $Tv_i = rv_i$ for each i.

Proof

We first deal with $n = 1$, so $v \in M$. Since M is semisimple, write $M = Rv \oplus N$ and let $P \in S$ be the projection of M into N along Rv. Notice that $PTv = TPv = Tv$ (since $T \in \mathrm{end}_S(M)$, T commutes with elements of S). Thus $Tv \in Rv$, and as such $Tv = rv$ for some $r \in R$.

We now reduce the general case to the case of $n = 1$. Consider the semisimple R-module M^n, and $(v_1, \ldots, v_n) \in M^n$. And consider $T^{\oplus n}\colon (m_1, \ldots, m_n) \mapsto (Tm_1, \ldots, Tm_n)$. We want to show that $T^{\oplus n}$ is in $\mathrm{end}_{\mathrm{end}_R(M^n)}(M^n)$.

Notice that there is an isomorphism $\mathrm{end}_R(M^n) \cong M_n(S)$. Indeed, to $F \in \mathrm{end}_R(M^n)$ we can define the matrix $[F]_{ij} = \iota_j \circ F \circ \pi_i$ ($\pi_i\colon M^n \to M$ the ith projection, and $\iota_i\colon M \to M^n$ the ith inclusion). Then since $T^{\oplus n}$ is scalar multiplication by an element of $S = \mathrm{end}_R(M)$, it commutes with matrices. That is to say, $T^{\oplus n} \in \mathrm{end}_{\mathrm{end}_R(M^n)}(M^n)$.

So by the $n = 1$ case, there is an $r \in R$ such that $T^{\oplus n}(v_1, \ldots, v_n) = r(v_1, \ldots, v_n)$ which is precisely what we want. ■

2.3.2 Corollary

Let M be a semisimple R-module, and let $S = \mathrm{end}_R(M)$. If M is finitely generated as an S-module, then $R \to \mathrm{end}_S(M)$ (defined by mapping r to scalar multiplication by r) is surjective.

Proof

Let $T_r\colon M \to M$ be scalar multiplication by r. Clearly $T_r \in \mathrm{end}_S(M)$ since for $F \in S$, $T_r(Fm) = rFm = Frm = FT_rm$.

Now suppose that $v_1, \ldots, v_n$ generate M. Then given $T \in \mathrm{end}_S(M)$, we know that there exists an $r \in R$ such that $Tv_i = rv_i$. But since $v_1, \ldots, v_n$ generate M, this extends to all of M: $T = T_r$, as required. ■

Let E be a simple R-module, and let $D_E = \mathrm{end}_R(E)$. Recall that D_E is a division ring by Schur. Then define

$$\mathcal{F}_E\colon R \to \mathrm{end}_{D_E}(E)$$

the natural map which maps $r \in R$ to multiplication by r on E. This is clearly a ring morphism.

2.3.3 Theorem (Artin-Wedderburn)

Let R be semisimple, then R has finitely many simple R-modules up to isomorphism. Furthermore, every simple R-module E is finite dimensional over D_E. Let $E_1, \dots, E_n$ list all non-isomorphic simple R-modules, then the ring morphism

$$\mathcal{F}\colon R \to \prod_{i=1}^{n} \operatorname{end}_{D_{E_i}}(E_i)$$

given by the product $\mathcal{F}_{E_1} \times \cdots \times \mathcal{F}_{E_n}$ is an isomorphism.

Proof

As already discussed, a semisimple ring is Artinian and thus has finitely many simple modules up to isomorphism. $\mathcal{F}$ is injective: if $\mathcal{F}(r) = 0$, then r acts as zero on every simple R-module, and thus as zero on every finitely generated semisimple R-module (as they are the finite sums of simple R-modules). In particular, it is zero in R.

We now claim $\mathcal{F}$ is surjective. Let us define $E = E_1 \oplus \cdots \oplus E_n$, and let $S = \operatorname{end}_R(E)$. We know that

$$S = \operatorname{end}_R(E) \cong \prod_{i,j=1}^{n} \hom_R(E_i, E_j)$$

by mapping $(\phi_{ij})_{ij}$ on the right to $\phi(e_1, \dots, e_n) = (\sum_i \phi_{i1}(e_i), \dots, \sum_i \phi_{in}(e_i))$. By Schur we then have

$$S \cong \prod_{i=1}^{n} \hom_R(E_i, E_i) = \prod_{i=1}^{n} D_{E_i}$$

Now, notice that we have a ring morphism

$$\operatorname{end}_{D_{E_1}}(E_1) \times \cdots \times \operatorname{end}_{D_{E_n}}(E_n) \to \operatorname{end}_S(E)$$

which maps $(T_1, \dots, T_n)$ to $T(e_1, \dots, e_n) = (T_1 e_1, \dots, T_n e_n)$. We claim that this is an isomorphism. Indeed it is clearly injective, we now show it is surjective. Let $T \in \operatorname{end}_S(E)$, and define $T_i = \pi_i \circ T \circ \iota_i$ where $\iota_i\colon E_i \to E$ is the inclusion morphism and $\pi_i\colon E \to E_i$ is the projection morphism. Then $(T_i)_i$ are mapped to the morphism $\bar{T}$:

$$(e_1, \dots, e_n) \mapsto (T_1 e_1, \dots, T e_n) = (\pi_i T \iota_1 e_1, \dots, \pi_n T \iota_n e_n)$$

Now consider $\Phi_i \in S$ which is the identity on the ith component and 0 everywhere else. We know that $\Phi_i T = T \Phi_i$ and $\pi_i \Phi_i = \pi_i$ and $\iota_i e_i = \Phi_i \bar{e}$. Putting this together we have

$$\pi_i \bar{T} \bar{e} = \pi_i T \iota_i e_i = \pi_i T \Phi_i \bar{e} = \pi_i \Phi_i T \bar{e} = \pi_i T \bar{e}$$

That is, $\pi_i \bar{T} = \pi_i T$ for all i, so $\bar{T} = T$ as required.

So we have that

$$\operatorname{end}_S(E) \cong \prod_{i=1}^{n} \operatorname{end}_{D_{E_i}}(E_i)$$

Now, our map $\mathcal{F}$ can be identified with the natural map $R \to \operatorname{end}_S(E)$. We know that this map is surjective for E semisimple and finitely generated as an S-module. E is clearly semisimple since it is the finite direct product of simple modules. To show that E is finitely generated, it is sufficient to show that E_i is finitely generated as a D_{E_i}-module.

Indeed, let E be a simple R-module. We want to show that E is a finitely generated D_E-module. Notice that $E \cong \hom_R(R, E)$ (which maps e to the map $\phi(1) = e$). So a D_E structure on E corresponds to a D_E structure on $\hom_R(R, E)$ where $d \in D_E$ and $\phi \in \hom_R(R, E)$, d acts on ϕ by $d \circ \phi$. R is semisimple and as such it is isomorphic to a finite direct sum of simple R-modules, let $R = R_1 \oplus \cdots \oplus R_k$. Then $\hom_R(R, E) \cong \prod_{i=1}^{k} \hom_R(R_i, E_i)$ as D_E modules. It is therefore sufficient to show that $\hom_R(R_i, E)$ is finitely generated. By Schur it is either zero or isomorphic to $\hom_R(E, E) = D_E$ which is finitely generated as a D_E module obviously. ■

2.3.4 Corollary (Artin-Wedderburn)

A ring is semisimple if and only if it is isomorphic to a finite product of matrix rings over division algebras.

Proof

Indeed, $\mathrm{end}_{D_E}(E)$ can be viewed as a matrix ring, since E is finitely generated over D_E, it is isomorphic to $M_n(D_E^{\mathrm{op}})$ where $n = \dim_{D_E} E$. Conversely a matrix ring over a division ring is semisimple ($M_n(D) \cong \mathrm{end}_D(D^n)$ which we saw was semisimple), and the finite product of semisimple rings is semisimple. ■

2.3.5 Proposition

Let R be a semisimple ring, and $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$. Then the division rings D_i and dimensions n_i are unique up to isomorphism.

2.4 The Jacobson radical

Note that our Fourier transform can be extended to all rings R. Indeed, we know that the set of isomorphism classes of simple modules over R is indeed a set (in bijection with the class of maximal ideals of R). So let $\mathfrak{S}_R$ be the set of simple R-modules, and we can consider

$$\mathcal{F}\colon R \to \prod_{E \in \mathfrak{S}_R} \mathrm{end}_{D_E}(E)$$

defined as before.

If R is not semisimple, then $\mathcal{F}$ may have a nontrivial kernel. That is, there may be a nonzero $r \in R$ which acts trivially on all simple R-modules.

2.4.1 Definition

The **(left) Jacobson radical** of R is the subset $J(R) \subseteq R$ consisting of all $r \in R$ for which $rE = 0$ for all simple R-modules E.

2.4.2 Lemma

(1) The Jacobson radical is a two-sided ideal in R.

(2) The Jacobson radical is equal to the intersection of all maximal left ideals in R.

(3) Let $x \in R$, then $x \in J(R)$ iff $1 - yx$ is left-invertible for all $y \in R$.

Proof

(1) Clearly $J(R)$ is a left ideal. It is a right ideal because if $xE = 0$ then $xrE = 0$ as well ($rE \subseteq E$).

(2) Let $\mathfrak{M}_R$ be the set of all maximal left ideals in R. We know that every maximal left ideal in R is of the form $\mathrm{ann}_R(e) = \{r \in R \mid re = 0\}$ for nonzero $e \in E$ where E is simple. (This was proven a while back.) Now, $x \in J(R)$ if and only if it is in the annihlator of every simple R-module E. That is, $x \in J(R)$ iff it is in $\mathrm{ann}_R(e)$ for every $e \in E$ for e nonzero and E simple. Equivalently, $x \in J(R)$ iff it is every maximal left ideal, as required.

(3) Note that $y \in R$ is left-invertible if and only if the left ideal generated by y is all of R. Equivalently, $y \in R$ is left-invertible iff it is not contained in any maximal left ideal. So suppose $x \in J(R)$ and $y \in R$, then $1 - yx$ cannot be in any maximal left ideal (let I be a maximal ideal, then $x \in I$ so $yx \in I$, and so if $1 - yx \in I$ we get $1 \in I$, a contradiction). Thus $1 - yx$ is left invertible.

Conversely suppose $x \notin J(R)$, then there exists a maximal ideal I such that $x \notin I$. Then $Rx + I = R$, so there exists a $y \in R, z \in I$ such that $yx + z = 1$, i.e. $z = 1 - yx$. But z is not left-invertible, so $1 - yx$ isn't. ■

2.4.3 Proposition

Let R be a ring, then the following are equivalent:

(1) R is semisimple,

(2) R is left Artinian and $J(R) = 0$.

Proof

If R is semisimple, we already know it is Artinian. Furthermore, $J(R) = \ker \mathcal{F}$ which is an isomorphism so $J(R) = 0$.

So now assume that R is Artinian and $J(R) = 0$. Since R is Artinian, it has a minimal left ideal $I_1 \subseteq R$, which is thus a simple submodule. Since $J(R) = 0$, there is a maximal left ideal $\mathfrak{m} \subseteq R$ which does not include I_1. Since I_1 is simple, $I_1 \cap \mathfrak{m} = 0$ and thus $R = I_1 \oplus \mathfrak{m}$. If $\mathfrak{m} = 0$ then we are finished, otherwise find a simple submodule $I_2 \subseteq \mathfrak{m}$ and a maximal left ideal $\mathfrak{n} \subseteq R$ such that $R = I_2 \oplus \mathfrak{n}$. Then $\mathfrak{m} = I_2 \oplus (\mathfrak{n} \cap \mathfrak{m})$, and so $R = I_1 \oplus I_2 \oplus (\mathfrak{m} \cap \mathfrak{n})$. We can proceed, with $R = I_1 \oplus \cdots \oplus I_n \oplus J_n$ with $J_{n+1} \subseteq J_n$. Since R is Artinian, eventually $J_n = 0$ and we will have finished. ■

2.4.4 Example

$\mathbb{Z}$ and $\mathbb{F}[X]$ are rings whose Jacobson radical is zero, but aren't semisimple (equivalently, not left Artinian).

Note that a simple R-module E can be seen as a $R/J(R)$-module. Indeed, $J(R) \subseteq \operatorname{ann}_R(E)$ so we can define $(x + J(R))e = xe$, so every simple R-module can also be seen as a $R/J(R)$-module. Since $R/J(R)$ is a quotient of R, every $R/J(R)$-module is also an R-module. Now let E be a simple R-module, and as such it is a $R/J(R)$-module. It is simple as an $R/J(R)$-module: if $F \subseteq E$ is an $R/J(R)$-submodule, then it is also an R-module and thus is trivial. Now if E is a simple $R/J(R)$-module, then let $F \subseteq E$ be an R-submodule. Since $\operatorname{ann}_R(E) \subseteq \operatorname{ann}_R(F)$, $J(R) \subseteq \operatorname{ann}_R(F)$ and so F is also a $R/J(R)$-module, and as such is trivial. So E is a simple R-module.

So we have shown

2.4.5 Proposition

R and $R/J(R)$ have the same simple modules.

2.4.6 Corollary

Let R be a ring, then $J(R/J(R)) = 0$.

Proof

We know that $J(R/J(R))$ is the intersection of all the annihlators of $R/J(R)$-simple modules. Since an $R/J(R)$-simple module is just an R-simple module, we get

$$J(R/J(R)) = \bigcap_E \operatorname{ann}_{R/J(R)}(E)$$

where the intersection is over all the simple R-modules. We know $(r+J(R))e = re$, and as such $\operatorname{ann}_{R/J(R)}(E)$ is equal to $\{r + J(R) \mid r \in \operatorname{ann}_R(E)\}$. This means that the intersection of all these annihlators is precisely $J(R)$. So $J(R/J(R)) = 0$ (since $J(R) = 0$ in $R/J(R)$). ■

2.4.7 Corollary

If R is left Artinian, then $R/J(R)$ is semisimple.

Proof

$R/J(R)$ is left Artinian, and we showed its Jacobson radical is zero. ■

2.4.8 Corollary

Let R be a left Artinian ring and $E_1, \ldots, E_n$ list all non-isomorphic simple R-modules. Then the ring morphism

$$\mathcal{F}\colon R \to \prod_{i=1}^{n} \operatorname{end}_{D_{E_i}}(E_i)$$

is surjective.

Proof

We know that $\mathcal{F}$ quotients over its kernel, which is $J(R)$. This quotient is precisely the Fourier transform of $R/J(R)$, which is semisimple. (This is because $E_1, \ldots, E_n$ list all the simple $R/J(R)$-modules too.) Since the Fourier transform of a semisimple ring is an isomorphism, the quotient is surjective, and thus so too is $\mathcal{F}$. ■

2.4.9 Lemma (Nakayama)

Let M be a finitely generated R-module. If $J(R)M = M$ then $M = 0$.

Proof

Let $v_1, \ldots, v_n$ generate M as an R-module, so $M = Rv_1 + \cdots + Rv_n$. We know that $J(R)M = M$, and so $M = J(R)Rv_1 + \cdots + J(R)Rv_n$. $J(R)$ is a two-sided ideal, so $M = J(R)v_1 + \cdots + J(R)v_n$. In particular $v_1 = x_1v_1 + \cdots + x_nv_n$ for $x_i \in J(R)$, and so $(1 - x_1)v_1 = x_2v_2 + \cdots + x_nv_n$. But since $1 - x_1$ is left invertible as $x_1 \in J(R)$, we get $v_1 \in Rv_2 + \cdots + Rv_n$. And so $v_2, \ldots, v_n$ generates M. We can then continue and iteratively remove vectors from this generating set to see that M is generated by the empty set, $M = 0$. ■

2.4.10 Proposition

(1) Every nilpotent left ideal in R is contained in $J(R)$.

(2) If R is left Artinian, then $J(R)$ is nilpotent.

Proof

(1) Let $I \subseteq R$ be a nilpotent ideal, i.e. $I^n = 0$. Let E be a simple R-module, then if $IE \neq 0$, since E is simple we obtain $IE = E$. (Note that $IE = \left\{ \sum_{j=1}^n i_j e_j \;\middle|\; i_j \in I, e_j \in E \right\}$.) But then inductively $I^k E = E$, and in particular $0 = I^n E = E$, a contradiction. So $IE = 0$ and thus $I \subseteq \operatorname{ann}_R(E)$, and so $I \subseteq J(R)$ as required.

(2) Consider $J(R)^n$ for $n \geq 1$. They form a decreasing sequence, and since R is left Artinian, must be finite. That is $J(R)^{n+k} = J(R)^n$ for some n and all $k \geq 0$. Let $I = J(R)^n$, we claim that it is zero. Notice that we have $J(R)^k I = J(R)^{n+k} = I$ for all $k \geq 0$, in particular for $k = 1$: $J(R)I = I$ and $k = n$: $II = I$.

So let us assume that $I \neq 0$. Let $\mathcal{J}$ be the set of left ideals $J \subseteq R$ for which $IJ \neq 0$. $\mathcal{J}$ is nonempty (since it contains R), and since R is Artinian, contains minimal elements. Let $J_0 \in \mathcal{J}$ be minimal. Notice that $IJ_0 \in \mathcal{J}$ since $I(IJ_0) = IIJ_0 = IJ_0 \neq 0$, and since $IJ_0 \subseteq J_0$ we must have $J_0 = IJ_0$. Then we have $J(R)J_0 = J(R)(IJ_0) = IJ_0 = J_0$. Now if we can show that J_0 is finitely generated, by Nakayama we have $J_0 = 0$, a contradiction.

Since $IJ_0 \neq 0$, let $x \in J_0$ such that $Ix \neq 0$, and thus $Rx \in \mathcal{J}$. By J_0's minimality, $Rx = J_0$, so J_0 is indeed finitely generated and we are finished. ■

2.4.11 Corollary

If R is commutative then $J(R)$ contains all nilpotent elements. If R is Artinian, then every element in $J(R)$ is nilpotent. Therefore if R is commutative and Artinian, $J(R)$ contains precisely all nilpotent elements.

Proof

Let $x \in R$ be nilpotent. Then $Rx \subseteq R$ is a nilpotent ideal: if $x^n = 0$ then $(rx)^n = r^n x^n = 0$ for all $rx \in Rx$. Thus by above $x \in Rx \subseteq J(R)$ as required.

If R is Artinian, then $J(R)$ is itself nilpotent, and as such for every $x \in J(R)$, $x^n \in J(R) = 0$. So x is nilpotent. ■

Now, let R be a finite-dimensional $\mathbb{F}$-alegbra. Given $x \in R$ consider the $\mathbb{F}$-linear transformation $m_x \colon R \to R$ given by $y \mapsto xy$. Let $\operatorname{tr}_R(x)$ be the trace of this linear transformation (which is well-defined as in linear algebra). Then define the function

$$(\bullet, \bullet) \colon R \times R \to R, \qquad (x, y) = \operatorname{tr}_R(xy)$$

This is a symmetric bilinear form: this is because $m_{xy} = m_x m_y, m_{x+y} = m_x + m_y, m_{\alpha x} = \alpha m_x$ (and $\operatorname{tr}_R(m_x m_y) = \operatorname{tr}(m_y m_x)$). The **radical** (or **kernel**) of a bilinear form is given by

$$\{x \in R \mid (x, y) = 0 \text{ for all } y \in R\}$$

2.4.12 Proposition

Suppose R is a finite-dimensional $\mathbb{F}$-algebra. Then $J(R)$ is contained in the radical of the symmetric bilinear form $(x, y) = \mathrm{tr}_R(xy)$. In particular, if this bilinear form is nondegenerate then R is semisimple.

Proof

Since R is a finite-dimensional $\mathbb{F}$-algebra it is Artinian (submodules are $\mathbb{F}$-spaces), and so $J(R)$ is nilpotent, and thus contains only nilpotent elements. Let $x \in J(R)$ then for any $y \in R$ we have $xy \in J(R)$, and so xy is nilpotent. This means that m_{xy} is nilpotent, and so $\mathrm{tr}_R(xy) = \mathrm{tr}(m_{xy}) = 0$. So x is in the radical of the bilinear form.

If the bilinear form is nondegenerate, then its radical is zero, and thus $J(R) = 0$. Since R is Artinian, this means R is semisimple. ■

Now we can prove Maschke once more!

Proof (Maschke)

We recall that G is a finite group and $|G| \in \mathbb{F}^\times$. We want to show finite dimensional representations over G are semisimple. Since G-representations can be thought of $\mathbb{F}[G]$-modules, it is sufficient to show that finite-dimensional $\mathbb{F}[G]$-modules are semisimple. A finite-dimensional $\mathbb{F}[G]$-module is a quotient of $\mathbb{F}[G]^n$, which is semisimple if $\mathbb{F}[G]$ is. Thus it is sufficient to prove that $\mathbb{F}[G]$ is semisimple.

By the above proposition, it is sufficient to show that the bilinear form $(x, y) = \mathrm{tr}_{\mathbb{F}[G]}(xy)$ is nondegenerate. Given $g \in G$, $m_{\delta_g}(\delta_h) = \delta_{gh}$, which means that the matrix representation of m_{δ_g} is a permutation matrix. This permutation has no fixed points if $g \neq 1$ and is the identity if $g = 1$. As such $\mathrm{tr}_{\mathbb{F}[G]}(\delta_g) = 0$ if $g \neq 1$ and $\mathrm{tr}_{\mathbb{F}[G]}(\delta_1) = |G|$. All in all, we have

$$\left(\sum_g c_g \delta_g, \delta_h\right) = \sum_g c_g \mathrm{tr}_{\mathbb{F}[G]}(\delta_{gh}) = |G| c_{h^{-1}}$$

So if $x = \sum_g c_g \delta_g \neq 0$, let $c_g \neq 0$, and then $(x, c_{g^{-1}}) \neq 0$. So the bilinear form is indeed non-degenerate, as required. ■

3 Tensor Products

3.1 The basic definition

Recall that what we have until now called a R-module is actually a *left* R-module. A right R-module is defined in much the same way, but multiplication is defined as a function $M \times R \to M$. While a left R-module is equivalent to a ring morphism $R \to \mathrm{end}(M)$, a right R-module is equivalent to a ring morphism $R^{\mathrm{op}} \to \mathrm{end}(M)$ (where $\mathrm{end}(M)$ is the ring of endomorphisms on the Abelian group M). So a right R-module is equivalent to a left R^{op}-module.

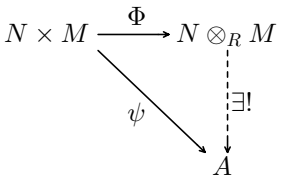
We also write ${}_RM$ to mean M is a left R-module and N_R to mean N is a right R-module.

3.1.1 Definition

Let M be a left R-module, and N a right R-module, and A an Abelian group. A biadditive map $\Phi\colon N \times M \to A$ (meaning it is additive in both of its components) is **balanced** (or **R-balanced**) if for all $n \in N, m \in M, r \in R$:

$$\Phi(nr, m) = \Phi(n, rm)$$

Let ${}_RM$ and N_R be R-modules. We define their *tensor product* to be an Abelian group $N \otimes_R M$ as well as a balanced biadditive map $\Phi\colon N \times M \to N \otimes_R M$ which satisfies the following the following *universal property*: for any Abelian group A and a balanced biadditive map $\psi\colon N \times M \to A$, there exists a unique Abelian group morphism $f\colon N \otimes_R M \to A$ such that $\psi = f \circ \Phi$. In a diagram:

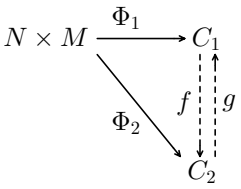


Φ should be thought of part of the structure of the tensor product, but it is usually left implicit and instead of writing $\Phi(n, m)$ one writes $n \otimes m$.

Now we can ask two questions: does such a construction exist, and if so is it unique? The answer to both is positive (for the latter, it is true of course up to isomorphism). We will show that the tensor product is unique.

First, notice that by taking $A = N \otimes_R M$ and $\psi = \Phi$ we see that $f = \mathrm{id}$ makes the diagram above commute. But f is unique; it is the *only* function which can make the diagram commute. Which means that if $\Phi = f \circ \Phi$ then $f = \mathrm{id}$.

Now suppose C_1, C_2 both satisfy the universal property for tensor products. Then the following diagram commutes (i.e. all compositions from the same source to the same destination are equal):



In particular, we have $\Phi_1 = (g \circ f) \circ \Phi_1$ and $\Phi_2 = (f \circ g) \circ \Phi_2$. But as said earlier, this means $g \circ f$ and $f \circ g$ are their respective identities, so f, g are isomorphisms: $C_1 \cong C_2$.

So all that remains is to show that an Abelian group with the universal property exists. To do so we will explicitly construct an Abelian group with the universal property. Given N, M we consider the free Abelian group over their product: $\mathbb{Z}[N \times M]$. Let us write $\delta_{(n,m)}$ for the element of the basis corresponding to $(n, m) \in N \times M$. We will construct $N \otimes_R M$ to be a quotient of this free group. In particular, we will have $\Phi(n, m) = [\delta_{(n,m)}]$.

In order for Φ to be a biadditive balanced morphism, this means our quotient must satisfy:

$$\begin{aligned}
\Phi(n_1 + n_2, m) = \Phi(n_1, m) + \Phi(n_2, m) &\Longrightarrow [\delta_{(n_1+n_2,m)}] = [\delta_{(n_1,m)}] + [\delta_{(n_2,m)}] \\
\Phi(n, m_1 + m_2) = \Phi(n, m_1) + \Phi(n, m_2) &\Longrightarrow [\delta_{(n,m_1+m_2)}] = [\delta_{(n,m_1)}] + [\delta_{(n,m_2)}] \\
\Phi(nr, m) = \Phi(n, rm) &\Longrightarrow [\delta_{(nr,m)}] = [\delta_{(n,rm)}]
\end{aligned}$$

This means that our quotient must contain all elements of the form

$$\delta_{(n_1+n_2,m)} - \delta_{(n_1,m)} - \delta_{(n_2,m)}, \qquad \delta_{(n,m_1+m_2)} - \delta_{(n,m_1)} - \delta_{(n,m_2)}, \qquad \delta_{(nr,m)} - \delta_{(n,rm)}$$

It turns out that taking these relations is sufficient, that is let us define K to be the subgroup generated by these elements, then we define

$$N \otimes_R M = \mathbb{Z}[N \times M]/K$$

and as discussed, $\Phi(n, m) = [\delta_{(n,m)}] = \delta_{(n,m)} + K$.

The relations given were sufficient for making Φ biadditive and balanced, so this construction is a valid contender for the tensor product. And it satisfies the universal property.

3.2 Basic cases

Now let us consider the tensor product of direct sums. That is, given $(N_i)_{i \in I}$ right R-modules and $(M_j)_{j \in J}$ left R-modules, consider the tensor product of

$$M \otimes_R N = \left(\bigoplus_{i \in I} N_i \right) \otimes_R \left(\bigoplus_{j \in J} M_j \right)$$

We claim that it is isomorphic to

$$\bigoplus_{i \in I, j \in J} N_i \otimes_R M_j$$

All we need to do is show that this has the universal property.

Take $\Phi\colon N \times M \to \bigoplus_{i,j} N_i \otimes_R M_j$ as $\Phi(n_i, m_j) = n_i \otimes m_j$ where $n_i \in N_i, m_j \in M_j$. This extends linearly: for $r_i, s_j \in R$ (all but finitely many being zero):

$$\Phi\left(\sum_{i\in I} n_i r_i, \sum_{j\in J} s_j m_j\right) = \sum_{i\in I, j\in J} (n_i r_i) \otimes (s_j m_j)$$

This is balanced: clearly this needs only be checked on elements of N_i, M_j: $\Phi(nr, m) = (nr) \otimes m = n \otimes (rm) = \Phi(n, rm)$. So Φ is biadditive and balanced. Notice that $\Phi_{ij} = \pi_{ij} \circ \Phi \circ \iota_{ij}$.

Now, suppose $\psi\colon N \times M \to A$ is also biadditive and balanced. Then we want an f such that $\psi = f \circ \Phi$. Note that we have a unique f_{ij} such that $\psi \circ \iota_{ij} = f_{ij} \circ \Phi_{ij} = f_{ij} \circ \pi_{ij} \circ \Phi \circ \iota_{ij}$. Further notice that if such an f exists,

$$f \circ \iota_{ij}^{\otimes} \circ \pi_{ij} \circ \Phi \circ \iota_{ij} = f \circ \Phi \circ \iota_{ij} = \psi \circ \iota_{ij}$$

So $f \circ \iota_{ij}^{\otimes}$ must be equal to f_{ij}. This uniquely determines f, and sastisfies the condition.

So we have shown:

3.2.1 Proposition

If $(N_i)_{i\in I}$ is a family of right R-modules, and $(M_j)_{j\in J}$ a family of left R-modules, then

$$\left(\bigoplus_{i\in I} N_i\right) \otimes_R \left(\bigoplus_{j\in J} M_j\right) \cong \bigoplus_{i\in I, j\in J} N_i \otimes_R M_j$$

3.2.2 Definition

Let R, S be rings. Then an (R, S)-**bimodule** is an Abelian group M which is both a left R-module and a right S-module, such that for all $r \in R, s \in S, m \in M$: $(rn)s = r(ns)$. We write that ${}_RM_S$ is a module.

In general a (R, S)-bimodule is equivalent to a ring morphism $R \times S^{\mathsf{op}} \to \mathrm{end}(M)$. Note that all left R-modules are $(R, \mathbb{Z})$-bimodules, and all right R-modules are $(\mathbb{Z}, R)$-bimodules.

So now suppose that ${}_SN_R$ and ${}_RM_T$ are modules. Then we claim that $N \otimes_R M$ is an (S, T)-bimodule.

Indeed, let $s \in S, t \in T$ and consider the map $N \times M \to N \otimes_R M$ by $(n, m) \mapsto (sn) \otimes (mt)$. This is clearly a biadditive balanced map. Thus we get a unique group morphism $N \otimes_R M \to N \otimes_R M$ such that $n \otimes m \mapsto (sn) \otimes (mt)$. So we have defined a function

$$S \times T^{\mathsf{op}} \to \mathrm{end}(N \otimes_R M)$$

and we readily check that this is a ring morphism.

That is to say, given modules ${}_SN_R, {}_RM_T$, their tensor product $N \otimes_R M$ is an (S, T)-bimodule. For special cases, if N or M is a one-sided module, then S or T can be considered to be $\mathbb{Z}$. For example, if ${}_SN_R$ is a bimodule but ${}_RM$ is a one-sided module, then considering it as ${}_RM_{\mathbb{Z}}$, we get that $N \otimes_R M$ is a $(S, \mathbb{Z})$-bimodule, or simply a left S-module.

In particular, if R is a commutative ring, there is no difference between left and right R-modules. So if N, M are R-modules (considered as (R, R)-bimodules), then $N \otimes_R M$ is an R-module.

Now, consider R a right R-module, then we claim that $R \otimes_R M \cong M$. Indeed, define $\Phi\colon R \times M \to M$ to be multiplication: $\Phi(r, m) = rm$. This is biadditive and balanced. Now for any Abelian group A and biadditive $\psi\colon R \times M \to A$, we want an $f\colon M \to A$ such that $\psi = f \circ \Phi$. I.e. $\psi(r, m) = f(rm)$. Since ψ is biadditive and balanced, we have $\psi(r, m) = \psi(1r, m) = \psi(1, rm)$. So define $f(m) = \psi(1, m)$, then $\psi(r, m) = \psi(1, rm) = f(rm)$ as required. Similarly we see that $M \otimes_R R \cong M$.

In particular, let $R = \mathbb{F}$ be a field. Then if N, M are $\mathbb{F}$-vector spaces, let $(n_i)_{i\in I}$ and $(m_j)_{j\in J}$ be bases. Then we have $N = \bigoplus_{i\in I} \mathbb{F}n_i$ and $M = \bigoplus_{j\in J} \mathbb{F}m_j$ and so by our above theorem:

$$N \otimes_{\mathbb{F}} M \cong \bigoplus_{(i,j)\in I\times J} (\mathbb{F}n_i) \otimes_{\mathbb{F}} (\mathbb{F}m_j)$$

Now, we know that $(\mathbb{F}n_i) \otimes_{\mathbb{F}} (\mathbb{F}m_j) \cong \mathbb{F} \otimes_{\mathbb{F}} \mathbb{F} \cong \mathbb{F}$. So this is isomorphic to $\bigoplus_{I\times J} \mathbb{F}$. Furthermore $\{n_i \otimes m_j\}_{i,j}$ forms a basis for $N \otimes_{\mathbb{F}} M$.

3.2.3 Proposition

Let N, M be vector spaces with bases $(n_i)_i$ and $(m_j)_j$. Then $(n_i \otimes m_j)$ forms a basis of $N \otimes M$, and in particular one has

$$\dim(N \otimes M) = (\dim N)(\dim M)$$

Now, if R is commutative, then an R-bilinear map $N \times M \to U$ (where U is an R-module), is in particular balanced. In the case of a commutative R, the universal property for tensor products is equivalent to the following universal property. Given an R-module U and an R-bilinear map $\psi: N \times M \to U$, there exists a unique R-module morphism $T: N \otimes_R M \to U$ such that $T(n \otimes m) = \psi(n, m)$. That is, when our ring is commutative, we can consider the universal property as a property of only R-modules (and not Abelian groups in general).

3.3 Basic properties

Let $\mathbb{F}$ be a field, and V, W be $\mathbb{F}$-vector spaces. Consider the dual space of V, $V^\vee = \hom_\mathbb{F}(V, \mathbb{F})$. Now, we have a $\mathbb{F}$-bilinear map $V^\vee \times W \to \hom_\mathbb{F}(V, W)$ defined by $(\phi, w) \mapsto [v \mapsto \phi(v)w]$. So by the universal property, there exists a unique $\mathbb{F}$-morphism $T: V^\vee \otimes_\mathbb{F} W \to \hom_\mathbb{F}(V, W)$ such that $T(\phi \otimes w) = [v \mapsto \phi(v)w]$.

3.3.1 Proposition

If V is finite-dimensional then the above $\mathbb{F}$-linear map $T: V^\vee \otimes_\mathbb{F} W \to \hom_\mathbb{F}(V, W)$ is an isomorphism.

Proof

Let $(e_i)_{i \in I}$ be a basis for V, and let $(e_i^*)_{i \in I}$ be its dual basis in $V^\vee$. Let $(f_j)_{j \in J}$ be a basis for W, then $(e_i^* \otimes f_j)_{i,j}$ is a basis for $V^\vee \otimes_\mathbb{F} W$. The image of $e_i^* \otimes f_j$ under T is $T_{ij}: v \mapsto e_i^*(v) f_j$. It is uniquely defined as $T_{ij}: e_j \mapsto \delta_{ij} f_j$. This obviously is a basis for $\hom_\mathbb{F}(V, W)$. ■

3.4 Tensor products of representations

Let G be a group and $\mathbb{F}$ a field. We will consider G-representations over $\mathbb{F}$.

Let V, W be two G-representations over $\mathbb{F}$. Then consider the map $V \times W \to V \otimes_\mathbb{F} W$ by $(v, w) \mapsto (gv) \otimes (gw)$ for $g \in G$. This is bilinear and balanced. As such, there exists an endomorphism $f_g \in \mathrm{end}_\mathbb{F}(V \otimes_\mathbb{F} W)$ such that $(gv) \otimes (gw) = f_g(v \otimes w)$. This forms a group morphism: $f_1(v \otimes w) = v \otimes w$ so $f_1 = \mathrm{id}$ and $f_{gg'} = (gg'v) \otimes (gg'w) = f_g(f_{g'}(v \otimes w))$, so $f_{gg'} = f_g \circ f_{g'}$. Thus $g \mapsto f_g$ forms a representation in $V \otimes_\mathbb{F} W$.

3.4.1 Definition

Let V be a G-representation. We define its **dual representation** as $V^\vee$ (V's dual space), where for $g \in G$ and $\phi \in V^\vee$ we define $g\phi: v \mapsto \phi(g^{-1}v)$.

Notice that this corresponds to our previous representation of $\hom_\mathbb{F}(V, W)$ (where $g \star T(v) = gT(g^{-1}v)$), where $W = \mathbb{F}$, since $\mathbb{F}$ has a trivial representation.

In particular, consider the $\mathbb{F}$-linear map $T: V^\vee \otimes_\mathbb{F} W \to \hom_\mathbb{F}(V, W)$. The domain and codomain of this map are all G-representations. We see that

$$T(g(\phi \otimes w)) = T((g\phi) \otimes (gw)): v \mapsto (g\phi)(v)gw = \phi(g^{-1}v)gw = g\phi(g^{-1}v)w$$

While

$$g \star T(\phi \otimes w)(v) = gT(\phi \otimes w)(g^{-1}v) = g\phi(g^{-1}v)w$$

Thus T is a morphism of G-representations.

3.4.2 Corollary

If V is a finite-dimensional G-representation, then the G-representations $V^\vee \otimes_{\mathbb{F}} W$ and $\hom_{\mathbb{F}}(V, W)$ are isomorphic.

This isomorphism is actually natural.

4 Character Theory

We fix a finite group G and a field $\mathbb{F}$ whose characteristic does not divide the order of G.

4.1 Definition and orthogonality

Given a G-representation V, we will sometimes write g_V for the image of $g \in G$ in this representation (e.g. $g_V = \rho(g)$).

4.1.1 Definition

Let V be a finite-dimensional G-representation. The **character** of this representation is the function $\mathrm{ch}_V \in \mathrm{Set}(G, \mathbb{F})$ given by

$$\mathrm{ch}_V(g) = \mathrm{tr}(g_V)$$

i.e. $\mathrm{ch}_V(g)$ is the trace of g in V.

4.1.2 Definition

The space of **class functions** on G is the set $\mathrm{Set}(G, \mathbb{F})^{\mathrm{cl}} \subseteq \mathrm{Set}(G, \mathbb{F})$ consisting of all functions constant on conjugacy classes of G, that is functions $f \in \mathrm{Set}(G, \mathbb{F})$ such that $f(hgh^{-1}) = f(g)$ (equivalently $f(hg) = f(gh)$) for all $g, h \in G$.

Clearly every character of G is a class function: $\mathrm{ch}_V(hgh^{-1}) = \mathrm{tr}(h_V g_V h_V^{-1}) = \mathrm{tr}(g_V)$, since similar transformations have equal traces.

4.1.3 Example

Let $\chi \colon G \to \mathbb{F}^\times$ be a character (in the previous sense, a group homomorphism). Then $\mathrm{ch}_{\mathbb{F}_\chi} = \chi$.

4.1.4 Example

Let X be a finite G-set, and recall the standard G-representation on $\mathbb{F}[X]$. Using X as a basis, the representation matrix of $g \in G$ is its associated permutation matrix on X, a 1 on the diagonal corresponds to a fixed point of X under g. Thus, $\mathrm{ch}_{\mathbb{F}[X]}(g)$ is equal to the number of fixed points of g.

4.1.5 Definition

Notice that function multiplication on $\mathrm{Set}(G, \mathbb{F})$ can be defined pointwise: $(f_1 \cdot f_2)(g) = f_1(g) \cdot f_2(g)$. This restricts to multiplication in $\mathrm{Set}(G, \mathbb{F})^{\mathrm{cl}}$ (i.e. the pointwise product of two class functions is another class function).

4.1.6 Lemma

Let V, W be finite G-representations, then

$$\mathrm{ch}_{V\otimes W} = \mathrm{ch}_V \cdot \mathrm{ch}_W$$

We write $V \otimes W$ for $V \otimes_{\mathbb{F}} W$.

Proof

Let $(e_i)_{i\in I}$ be a basis for V and $(f_j)_{j\in J}$ a basis for W. Write $ge_i = \sum_{i'} c_{ii'}e_{i'}$ and $gf_j = \sum_{j'} d_{jj'}f_{j'}$. Then $(e_i \otimes f_j)_{i\in I, j\in J}$ is a basis for $V \otimes W$, and

$$g(e_i \otimes f_j) = ge_i \otimes gf_j = \left(\sum_{i'} c_{ii'}e_{i'}\right) \otimes \left(\sum_{j'} d_{jj'}f_{j'}\right) = \sum_{i',j'} c_{ii'}d_{jj'}e_{i'} \otimes f_{j'}$$

Thus

$$\mathrm{ch}_{V\otimes W}(g) = \mathrm{tr}_{V\otimes W}(g) = \sum_{i\in I, j\in J} c_{ii}d_{jj} = \sum_i c_{ii} \cdot \sum_j d_{jj} = \mathrm{ch}_V(g) \cdot \mathrm{ch}_W(g)$$

as required. ■

4.1.7 Definition

For a function $f \in \mathrm{Set}(G, \mathbb{F})$, define its **dual** $f^* \in \mathrm{Set}(G, \mathbb{F})$ by $f^*(g) = f(g^{-1})$. Note that this again restricts to class functions as well.

4.1.8 Lemma

Let V be a finite-dimensional G-representation, and let V^* be its dual space. Then $\mathrm{ch}_{V^*} = \mathrm{ch}_V^*$.

Proof

Let $(e_i)_{i\in I}$ be a basis for V and let $(e_i^*)_{i\in I}$ be its dual basis in V^*. Write $g^{-1}e_j = \sum_i c_{ji}e_i$. Then $ge_i^*(e_j) = e_i^*(g^{-1}e_j) = c_{ji}$, meaning $ge_i^* = \sum_j c_{ji}e_j^*$, so

$$\mathrm{ch}_{V^*}(g) = \sum_i c_{ii} = \mathrm{ch}_V(g^{-1})$$

as required. ■

4.1.9 Corollary

Let V, W be finite-dimensional G-representations. Then

$$\mathrm{ch}_{\hom(V,W)} = \mathrm{ch}_V^* \cdot \mathrm{ch}_W$$

Proof

This follows from the previous two lemmas, as $\hom(V,W) \cong V^* \otimes W$. ■

4.1.10 Definition

For $f \in \mathrm{Set}(G, \mathbb{F})$, define $\mathrm{Av}(f) \in \mathbb{F}$ by

$$\mathrm{Av}(f) = \frac{1}{|G|} \sum_{g \in G} f(g)$$

4.1.11 Lemma

For a finite-dimensional G-representation V: $\mathrm{Av}(\mathrm{ch}_V) = \dim V^G$.

Proof

Recall the averaging operator $\mathrm{Av}_V^G \colon V \to V$,

$$\mathrm{Av}_V^G(v) = \frac{1}{|G|} \sum_{g \in G} gv$$

As it is a projection operator on V^G, we have $\mathrm{tr}_V(\mathrm{Av}_V^G) = \dim V^G$. But

$$\mathrm{tr}_V(\mathrm{Av}_V^G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}_V(g) = \frac{1}{|G|} \sum_{g \in G} \mathrm{ch}_V(g) = \mathrm{Av}(\mathrm{ch}_V)$$

as required. ■

4.1.12 Definition

Define the symmetric bilinear form $(\bullet, \bullet)$ on $\mathrm{Set}(G, \mathbb{F})$ by

$$(f_1, f_2) = \mathrm{Av}(f_1^* \cdot f_2) = \frac{1}{|G|} \sum_{g \in G} f_1(g^{-1}) f_2(g)$$

This being symmetric and bilinear are obvious (for symmetry, note that $\mathrm{Av}(f) = \mathrm{Av}(f^*)$ and $(f_1^* \cdot f_2)^* = f_2^* \cdot f_1$).

4.1.13 Corollary

Let V, W be finite-dimensional G-representations. Then

$$\dim \hom_G(V,W) = (\mathrm{ch}_V, \mathrm{ch}_W)$$

Proof

Note that $\hom_G(V,W) = \hom(V,W)^G$ and as such

$$\dim \hom_G(V,W) = \mathrm{Av}(\mathrm{ch}_{\hom(V,W)}) = \mathrm{Av}(\mathrm{ch}_V^* \cdot \mathrm{ch}_W) = (\mathrm{ch}_V, \mathrm{ch}_W) \qquad \blacksquare$$

As such, we have almost immediately:

4.1.14 Corollary

Let E, F be irreducible G-representations. Then

$$(\mathrm{ch}_E, \mathrm{ch}_F) = \begin{cases} d_E & E \cong F \\ 0 & \text{else} \end{cases}$$

where $d_E \in \mathbb{Z}_{\geq 1}$ is the dimension of the division algebra $\mathrm{end}_G(E)$.

Proof

We know $(\mathrm{ch}_E, \mathrm{ch}_F) = \dim \hom_G(E,F)$. Since E, F are irreducible, by Schur $\hom_G(E,F) \cong \mathrm{end}_G(E)$ iff $E \cong F$ and $\hom_G(E,F) = 0$ otherwise. $\blacksquare$

Note that, depending on the characteristic of our field $\mathbb{F}$, we may have that $(\mathrm{ch}_E, \mathrm{ch}_F) = 0$ even if $E \cong F$ (since d_E may be 0 in $\mathbb{F}$). But if $\mathbb{F}$ is algebraically closed then we know $\mathrm{end}_G(E) \cong \mathbb{F}$, as such:

4.1.15 Corollary

Let E, F be irreducible G-representations over $\mathbb{F}$ algebraically closed. Then

$$(\mathrm{ch}_E, \mathrm{ch}_F) = \begin{cases} 1 & E \cong F \\ 0 & \text{else} \end{cases}$$

4.1.16 Corollary

If $\mathbb{F}$ is algebraically closed, and $E_1, \ldots, E_n$ be an exhaustive, non-isomorphic, list of all irreducible G-representations. Then $\mathrm{ch}_{E_1}, \ldots, \mathrm{ch}_{E_n} \in \mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$ are linearly independent.

Proof

Suppose $\sum_i c_i \mathrm{ch}_{E_i} = 0$, then by orthogonality we have

$$c_j = \left(\sum_i c_i \mathrm{ch}_{E_i}, \mathrm{ch}_{E_j} \right) = (0, \mathrm{ch}_{E_j}) = 0$$

so $\mathrm{ch}_{E_1}, \ldots, \mathrm{ch}_{E_n}$ are indeed linearly independent. $\blacksquare$

4.1.17 Theorem

If $\mathbb{F}$ is algebraically closed and $E_1, \ldots, E_n$ an exhaustive list of irreducible G-representations. Then $\mathrm{ch}_{E_1}, \ldots, \mathrm{ch}_{E_n}$ form a basis for $\mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$.

Proof

We showed that the characters of E_i are linearly independent. Furthermore, we showed earlier that $\dim \mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}} = n$ (which is equal to the number of conjugacy classes of G). Thus these characters must also span $\mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$, and as such they form a basis. ■

For functions $f_1, f_2 \in \mathrm{Set}(G,\mathbb{F})$ we define $f_1 + f_2$ pointwise as well. This again restricts to class functions. It is not hard to see that

$$\mathrm{ch}_{V\oplus W} = \mathrm{ch}_V + \mathrm{ch}_W$$

4.1.18 Proposition

Suppose $\mathbb{F}$ has characteristic 0. Let V, W be finite-dimensional G-representations. Then V is isomorphic to W if and only if $\mathrm{ch}_V = \mathrm{ch}_W$.

Proof

Clearly isomorphic G-representations have the same character. Conversely, suppose $\mathrm{ch}_V = \mathrm{ch}_W$. To show that $V \cong W$ it is sufficient to show that for every irreducible E, $[V : E] = [W : E]$ (since they are the sum of irreducibles). Note that we have

$$[V : E] = \dim \hom_G(V, E) = (\mathrm{ch}_V, \mathrm{ch}_E) = (\mathrm{ch}_W, \mathrm{ch}_E) = \dim \hom_G(W, E) = [W : E]$$

This is equality in $\mathbb{F}$, but since it has characteristic 0, it is equality in $\mathbb{Z}$ as well. ■

4.1.19 Proposition

Let E be an irreducible G-representation over algebraically closed $\mathbb{F}$. Then the characteristic of $\mathbb{F}$ does not divide $\dim_{\mathbb{F}} E$.

Proof

Let $f \in \mathrm{Set}(G,\mathbb{F})^{\mathsf{cl}}$ and define $d = \sum_{g\in G} f(g)\delta_g \in Z(\mathbb{F}[G])$. The action of d on E defines $T_d \in \mathrm{end}_G(E)$, and so by Schur T_d is scalar multiplication. Thus the trace of T_d is a multiple of $\dim_{\mathbb{F}} E$. If the characteristic of $\mathbb{F}$ divides this dimension, this would mean $\mathrm{tr}(T_d) = 0$. But

$$\mathrm{tr}(T_d) = \sum_{g\in G} f(g)\mathrm{ch}_E(g) = (f^*, \mathrm{ch}_E)$$

So let $f = \mathrm{ch}_E^*$, then we get $\mathrm{tr}(T_d) = (\mathrm{ch}_E, \mathrm{ch}_E) = 1$. But this contradicts $\mathrm{tr}(T_d) = 0$. ■

Recall that for an irreducible G-representation E over an algebraically closed field $\mathbb{F}$, we define $e_E \in Z(\mathbb{F}[G])$ which acts by the identity on E and 0 on all other non-isomorphic irreducible representations. Equivalently, e_E is the unique element whose action on every G-representation V is projection onto V_E. Recall that we had a formula for e_E in the commutative case.

4.1.20 Proposition

$$e_E = \frac{\dim_{\mathbb{F}} E}{|G|} \sum_{g\in G} \mathrm{ch}_E(g^{-1})\delta_g$$

Proof

We will take e_E to be this formula, and show that it has the desired property. Let F be an irreducible G-representation, given by the homomorphism $\rho\colon \mathbb{F}[G] \to \mathrm{end}_{\mathbb{F}}(F)$. Now, we have that $\rho(e_E) \in \mathrm{end}_G(F)$: (we show this for $e'_E = |G|/\dim_{\mathbb{F}} Ee_E$)

$$\rho(e'_E)\rho(\delta_h) = \sum_{g\in G} \mathrm{ch}_E(g^{-1})\rho(\delta_{gh}) = \sum_g \mathrm{ch}_E(hg^{-1})\rho(\delta_g) = \sum_g \mathrm{ch}_E(g^{-1}h)\rho(\delta_g)$$

which is $\rho(\delta_h)\rho(e'_E)$. Thus by Schur, $\rho(e_E)$ is scalar multiplication.
We showed that $\dim_{\mathbb{F}} F \neq 0$ in $\mathbb{F}$. As such, if $\mathrm{tr}(\rho(e_E)) = 0$ in $\mathbb{F}$, then $\rho(e_E) = 0$, and if $\mathrm{tr}(\rho(e_E)) = \dim_{\mathbb{F}} F$ then $\rho(e_E) = \mathrm{id}$. So we want to show that if F is not isomorphic to E then $\mathrm{tr}(\rho(e_E))$, and if $E \cong F$ then $\mathrm{tr}(\rho(e_E)) = \dim_{\mathbb{F}} E$. Indeed:

$$\mathrm{tr}(\rho(e_E)) = \frac{\dim_{\mathbb{F}} E}{|G|}\sum_{g\in G} \mathrm{ch}_E(g^{-1})\mathrm{tr}(\rho(g)) = \frac{\dim_{\mathbb{F}} E}{|G|}\sum_{g\in G} \mathrm{ch}_E(g^{-1})\mathrm{ch}_F(g) = \dim_{\mathbb{F}} E \cdot (\mathrm{ch}_E, \mathrm{ch}_F)$$

So we have the desired result. ■

Note that in the case $\mathbb{F} = \mathbb{C}$, we can also define the Hermitian form (inner product):

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

We claim that we have $(\mathrm{ch}_V, \mathrm{ch}_W) = \langle \mathrm{ch}_V, \mathrm{ch}_W\rangle$. Indeed, this is because $\mathrm{ch}_W(g^{-1}) = \overline{\mathrm{ch}_W(g)}$; consider the eigenvalues $\{\lambda_i\}_i$ (with multiplicity) of g_W, since $g_W^{|W|} = \mathrm{id}$, these are all roots of unity. As such $\lambda_i^{-1} = \overline{\lambda}_i$. The eigenvalues of g_W^{-1} are $\{\lambda_i^{-1}\}_i$, and thus

$$\mathrm{ch}_W(g^{-1}) = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda}_i = \overline{\sum_i \lambda_i} = \overline{\mathrm{ch}_W(g)}$$

The benefit of using the inner product is that it can generalize to topological groups on Hilbert spaces. The bilinear form has the benefit of generalizing to other fields.

4.1.21 Proposition

The bilinear form $(\bullet, \bullet)$ on $\mathrm{Set}(G, \mathbb{F})$, and its restriction to the set of class functions, is nondegenerate.

Proof

Let $f \in \mathrm{Set}(G, \mathbb{F})$. If $(f, f') = 0$ for all $f' \in \mathrm{Set}(G, \mathbb{F})$ then in particular we have $(f, \delta_g^*) = 0$ for all $g \in G$. But by definition

$$(f, \delta_g^*) = \frac{1}{|G|} f(g)$$

and so $f(g) = 0$ for all $g \in G$, so $f = 0$. So the bilinear form is non-degenerate on $\mathrm{Set}(G, \mathbb{F})$.
Now we consider its restriction to $\mathrm{Set}(G, \mathbb{F})^{\mathsf{cl}}$. Consider

$$\mathrm{Av}\colon \mathrm{Set}(G, \mathbb{F}) \to \mathrm{Set}(G, \mathbb{F})^{\mathsf{cl}}, \qquad \mathrm{Av}(f)(g) = \frac{1}{|G|}\sum_{h\in G} f(hgh^{-1})$$

We quickly check that this is a projection operator onto $\mathrm{Set}(G, \mathbb{F})^{\mathsf{cl}}$. Furthermore, we have

$$(\mathrm{Av}(f), f') = (f, \mathrm{Av}(f'))$$

Now suppose $f \in \mathrm{Set}(G, \mathbb{F})^{\mathsf{cl}}$ with $(f, f') = 0$ for all $f' \in \mathrm{Set}(G, \mathbb{F})^{\mathsf{cl}}$. Then for every $f' \in \mathrm{Set}(G, \mathbb{F})$ we have

$$(f, f') = (\mathrm{Av}(f), f') = (f, \mathrm{Av}(f')) = 0$$

And so $f = 0$ by the non-degeneracy of the bilinear form on $\mathrm{Set}(G, \mathbb{F})$. ■

4.2 Integral elements

We will assume that $\mathbb{F}$ is algebraically closed.

4.2.1 Definition

An element a in a ring R is **integral** if it is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

If $a \in S$ is integral and $S \subseteq R$, clearly $a \in R$ is integral.

4.2.2 Lemma

Let R be a ring and $a \in R$, then a is integral iff $\mathbb{Z}[a] \subseteq R$, defined to be the $\mathbb{Z}$-span of $\{1, a, a^2, \ldots\}$, is a finitely generated $\mathbb{Z}$-module.

Proof

If a is integral, then suppose $f \in \mathbb{Z}[x]$ is monic with $f(a) = 0$. Suppose its degree is n, then $a^n \in \operatorname{span}_{\mathbb{Z}} \{1, \ldots, a^{n-1}\}$, and so we see that the span of $\{1, a, \ldots\}$ is equal to the span of $\{1, \ldots, a^{n-1}\}$.

Conversely, suppose $\operatorname{span}_{\mathbb{Z}} \{a^k\}_k$ is finitely generated. Notice that $\mathbb{Z}[a]$ can be equivalently written as $\{f(a) \mid f \in \mathbb{Z}[x]\}$, and so if it is finitely generated, it can be generated by a set of the form $\{1, \ldots, a^{n-1}\}$ (take $n-1$ to be the maximum degree of polynomials in the generating set). So a^n can be expressed as a $\mathbb{Z}$-linear combination of elements $1, \ldots, a^{n-1}$, and so a is integral. ■

4.2.3 Corollary

Let R be a ring, finitely-generated as a $\mathbb{Z}$-module. Then all elements of R are integral.

Proof

Let $a \in R$, then $\mathbb{Z}[a] \subseteq R$ is a $\mathbb{Z}$-submodule. Since $\mathbb{Z}$ is Noetherian, submodules of finitely generated modules are also finitely generated. As such $\mathbb{Z}[a]$ is finitely generated; the result follows from the previous lemma. ■

4.2.4 Proposition

The subset of integral elements of a commutative ring is a subring.

Proof

Clearly $0, 1 \in R$ are integral. Now if $a, b \in R$ are integral, say $\mathbb{Z}[a] = \operatorname{span}_{\mathbb{Z}} \{1, \ldots, a^n\}$ and $\mathbb{Z}[b] = \operatorname{span}_{\mathbb{Z}} \{1, \ldots, b^m\}$. Then by commutativity, $\mathbb{Z}[a, b] = \operatorname{span}_{\mathbb{Z}} \{a^k b^\ell\}_{k \leq n, \ell \leq m}$ is finitely-generated. Now we clearly have $\mathbb{Z}[a+b], \mathbb{Z}[ab] \subseteq \mathbb{Z}[a, b]$, and since $\mathbb{Z}$ is Noetherian, these must be finitely-generated too. ■

4.2.5 Example

The subring of integral elements of $\mathbb{Q}$ is $\mathbb{Z}$.

A clear property of integral elements is that they are preserved under ring morphisms: if $a \in R$ is integral and $\phi \colon R \to S$ is a morphism, then $\phi(a) \in S$ is integral. In particular what this means is that every integer in a ring is integral. Explicitly, let $n \in \mathbb{Z}$, then n is clearly integral in $\mathbb{Z}$. Let $\phi \colon \mathbb{Z} \to R$ be the canonical morphism, then $\phi(n) \in R$ is integral.

4.2.6 Lemma

(1) Let $d = \sum_{g\in G} c_g\delta_g \in \mathbb{F}[G]$, and suppose that c_g are all integers. Then d is integral.

(2) Let $d = \sum_{g\in G} c_g\delta_g \in Z(\mathbb{F}[G])$, and suppose that c_g are all integral in $\mathbb{F}$. Then d is integral.

Proof

(1) d clearly lies in the obvious morphism $\mathbb{Z}[G] \to \mathbb{F}[G]$, and every element of $\mathbb{Z}[G]$ is integral since $\mathbb{Z}[G]$ is a finitely-generated $\mathbb{Z}$-module.

(2) Note that each δ_g is integral by the previous point, and $c_g \in \mathbb{F} \subseteq \mathbb{F}[G]$ are integral. $Z(\mathbb{F}[G])$ is commutative, and so its subring of integral elements forms a subring. Thus d must be integral, as the sum and product of integral elements. ■

4.2.7 Lemma

Let V be a finite-dimensional G-representation. Then for every $g \in G$, $\mathrm{ch}_V(g) \in \mathbb{F}$ is integral.

Proof

Since $g^n = 1$ in G, $g_V^n = \mathrm{id}_V$ for some n. Thus the eigenvalues of g_V are all roots of unity, which are clearly integral. Since $\mathrm{ch}_V(g)$ is the sum of these integral elements, and $\mathbb{F}$ is commutative, $\mathrm{ch}_V(g)$ must be integral. ■

4.2.8 Proposition

Let E be an irreducible G-representation, then $\dim E$ divides $|G|$.

Proof

We will prove this for the case that $\mathrm{char}\mathbb{F} = 0$.

Let $\rho\colon \mathbb{F}[G] \to \mathrm{end}(E)$ be the $\mathbb{F}$-algebra morphism corresponding to G's action on E. Recall the central idempotent

$$e_E = \frac{\dim E}{|G|} \sum_{g\in G} \mathrm{ch}_E(g^{-1})\delta_g \in Z(\mathbb{F}[G])$$

This acts by identity on E, and so

$$d = \sum_{g\in G} \mathrm{ch}_E(g^{-1})\delta_g \in Z(\mathbb{F}[G])$$

acts as multiplication by $\lambda = |G|/\dim E$ on E. Thus $\rho(d) = \lambda \mathrm{id}_E$ is integral in $\mathbb{F}\cdot\mathrm{id}_E \subseteq \mathrm{end}(E)$. Thus $\lambda \in \mathbb{F}$ (identified with $\rho(d) \in \mathbb{F}\cdot\mathrm{id}_E \cong \mathbb{F}$) is integral. So $\lambda = |G|/\dim E \in \mathbb{Q} \subseteq \mathbb{F}$ is integral, which means it must be an integrer, so $\dim E$ divides $|G|$. ■

We can strengthen this result.

4.2.9 Definition

Let V be a G-representation and W an H-representation. Their **outer tensor product** is the $G \times H$-representation $V \boxtimes_{\mathbb{F}} H$, whose base vector space is $V \otimes_{\mathbb{F}} H$, but with an action given by

$$(g,h)(v \otimes w) = (gv) \otimes (hw)$$

Note that if V, W are both G-representations then composing the diagonal morphism $G \to G \times G$ with the representation $G \times G \to \mathrm{end}(V \boxtimes_{\mathbb{F}} W)$ gives the canonical G-representation $V \otimes_{\mathbb{F}} W$.

4.2.10 Proposition

Let E_1, E_2 be irreducible representations of the finite groups G_1, G_2 respectively. Then $E_1 \boxtimes E_2$ is an irreducible representation of $G_1 \times G_2$.

Using this we can show

4.2.11 Proposition

Let E be an irreducible G-representation. Then $\dim E$ divides $[G : Z(G)]$.

Proof

Let us write $A = Z(G)$. For $m \geq 1$ consider the irreducible representation $E^{\boxtimes m} = E \boxtimes_{\mathbb{F}} \cdots \boxtimes_{\mathbb{F}} E$ of $G^m = G \times \cdots \times G$. Let us consider the subgroup A_m of A^m given by all tuples $(a_1, \ldots, a_m) \in A^m$ for which $a_1 \cdots a_m = 1$ (this is clearly a subgroup).

A acts on E by scalars (Schur), i.e. there exists a character $\chi \colon A \times \mathbb{F}^\times$ such that $a \cdot v = \chi(a)v$ for $a \in A, v \in E$. Then A^m acts on $E^{\boxtimes m}$ by $(a_1, \ldots, a_m) \cdot (v_1 \otimes \cdots \otimes v_m) = \chi(a_1 \cdots a_m)(v_1 \otimes \cdots \otimes v_m)$ (by linearity and χ being a morphism). This means that A_m acts trivially on $E^{\boxtimes m}$.

In general if H is a normal subgroup of G which acts trivially on V, then V can be given a natural G/H-representation, which preserves things like irreducibility. A_m, as a subgroup of A^m, in turn a subgroup of $Z(G^m)$, is normal in G^m. Thus $E^{\boxtimes m}$ has a natural G/A_m-representation, and is irreducible. Thus we have that $\dim E^{\boxtimes m} = (\dim E)^m$ divides $|G^m/A_m| = |G|^m/|A_m| = |G|^m/|A|^{m-1}$ (clearly by construction $|A_m| = |A|^{m-1}$).

Given a prime p and an integer n, let $v_p(n)$ be the number of times p divides n. Clearly we have $v_p(n^k) = kv_p(n)$ and if n divides m then $v_p(n) \leq v_p(m)$ (in general $v_p(nm) = v_p(n) + v_p(m)$), so

$$mv_p(\dim E) \leq v_p(|G|^m/|A|^{m-1}) = mv_p(|G|) - (m-1)v_p(|A|)$$

Thus

$$v_p(\dim E) \leq v_p(|G|/|A|) + \frac{1}{m}v_p(|A|) = v_p([G : Z(G)]) + \frac{1}{m}v_p(|A|)$$

Letting $m \to \infty$ we get $v_p(\dim E) \leq v_p([G : Z(G)])$ for all prime p. Thus we must have that $\dim E$ divides $[G : Z(G)]$. ∎

4.3 Burnside's Theorem

We will prove the following theorem:

4.3.1 Theorem (Burnside)

If G is a finite group whose order has at most two prime divisors, then G is solvable.

This theorem's statement does not mention representation at all, yet its proof will utilize it.
We will call integral elements of $\mathbb{C}$ *algebraic integers*.

4.3.2 Lemma

Let $\zeta_1, \dots, \zeta_n \in \mathbb{C}^\times$ be roots of unity, then

(1) The average $(\zeta_1 + \cdots + \zeta_n)/n$ has modulus in $[0, 1]$, and 1 is attained iff $\zeta_1 = \cdots = \zeta_n$.

(2) The average $(\zeta_1 + \cdots + \zeta_n)/n$ is an algebraic integer iff it is zero or $\zeta_1 = \cdots = \zeta_n$.

Proof

(1) Clearly we have $|(\zeta_1 + \cdots + \zeta_n)/n| \leq (|\zeta_1| + \cdots + |\zeta_n|)/n = 1$ with equality occurring meaning that all ζ_i are real scalar multiples of one another by Cauchy-Schwarz. Since these are roots of unity, they are real scalar multiples iff they differ only by sign. The result follows.

(2) By the previous point, it is sufficient to show that the average is an algebraic integer iff its modulus is 0 or 1. Let a be the average, suppose it is not zero, then consider the Galois extension $K = \mathbb{Q}[\zeta_1, \dots, \zeta_n]/\mathbb{Q}$ (it is Galois as it is the compositum of Galois extensions), which defines the norm

$$N \colon K^\times \to \mathbb{Q}^\times, \qquad N(x) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(x)$$

In particular, $N(a) \in \mathbb{Q}$. Furthermore, if a is an algebraic integer, so is every $\sigma(a)$, and thus so is $N(a)$ as their product. Therefore $N(a) \in \mathbb{Z}$, and is nonzero. Furthermore, $\sigma(a)$ must also be an average of roots of unity (since $\sigma(\zeta_i)$ is a root of unity), thus its modulus is in $[0, 1]$. Therefore the modulus (now absolute value) of $N(a)$ is in $[0, 1]$; since it is a nonzero integer it must be 1. Thus the modulus of every $\sigma(a)$ must be 1; in particular $|a| = 1$ as required. ■

We denote by C_g the conjugacy class of an element $g \in G$.

4.3.3 Lemma

Let E be an irreducible G-representation over $\mathbb{C}$. Let $g \in G$ and suppose that $|C_g|$ and $\dim E$ are relatively prime. Then either $\mathrm{ch}_E(g) = 0$ or g acts on E by scalar.

Proof

Let $\rho \colon \mathbb{C}[G] \to \mathrm{end}(E)$ be the $\mathbb{C}$-algebra morphism corresponding to G's action on E. Define

$$d = \sum_{h \in C_g} \delta_h \in Z(\mathbb{C}[G])$$

By Schur, $\rho(d)$ is scalar multiplication on E. Furthermore, d is an integral element, and so its image under ρ in $\mathbb{C} \cong \mathbb{C} \cdot \mathrm{id}_E \subset \mathrm{end}(E)$ is also an integral element. Its image under this correspondence (i.e. the scalar it multiplies by) is

$$\frac{\mathrm{tr}(\rho(d))}{\dim E} = \frac{|C_g| \mathrm{ch}_E(g)}{\dim E}$$

Now, since $|C_g|$ and $\dim E$ are relatively prime, this means that $\mathrm{ch}_E(g)/\dim E$ is integral. Indeed, 1 can be

expressed as a $\mathbb{Z}$-linear combination of $|C_g|$ and $\dim E$, suppose $1 = \alpha|C_g| + \beta \dim E$ then

$$\frac{\alpha|C_g|\mathrm{ch}_E(g)}{\dim E} = \frac{(1-\beta\dim E)\mathrm{ch}_E(g)}{\dim E} = \frac{\mathrm{ch}_E(g)}{\dim E} - \beta\mathrm{ch}_E(g)$$

So $\mathrm{ch}_E(g)/\dim E \in \mathbb{Z}[|C_g|\mathrm{ch}_E(g)/\dim E]$, meaning $\mathbb{Z}[\mathrm{ch}_E(g)/\dim E] = \mathbb{Z}[|C_g|\mathrm{ch}_E(g)/\dim E]$, which is finitely-generated and as such $\mathrm{ch}_E(g)/\dim E$ is integral.

Now, $\mathrm{ch}_E(g)/\dim E$ is the average of the eigenvalues of g_E; an average of roots of unity. This is integral iff $\mathrm{ch}_E(g) = 0$ or all of g_E's eigenvalues are equal. In the latter case, this means that g_E is multiplication by scalar. ■

4.3.4 Proposition

If G contains a conjugacy class in which the number of elements is a positive power of a prime number, then G is not simple.

Proof

Let $C_g \subseteq G$ be a conjugacy class whose order is a positive power of a prime p. We will show there exists a non-trivial irreducible G-representation E over $\mathbb{C}$ over which C_g's elements act by scalar multiplication (they all act by the same scalar, since they are conjugate). Then for $g \neq h \in C_g$ we have that gh^{-1} acts by identity, so the kernel of $\rho\colon G \to \mathrm{GL}(E)$ is a non-trivial proper normal subgroup of G; G is not simple.

By the previous lemma, it is sufficient to find a non-trivial irreducible G-representation E such that p does not divide $\dim E$ and $\mathrm{ch}_E(g) \neq 0$. Recall that (letting the sum run over irreducible G-representations):

$$\sum_E (\dim E)\cdot \mathrm{ch}_E(g) = 0$$

We split this sum up

$$1 + \sum_{p|\dim E} (\dim E)\mathrm{ch}_E(g) + \sum_{\neg p|\dim E} (\dim E)\mathrm{ch}_E(g) = 0$$

(The final sum also supposes that E is nontrivial.) This is an equation in the complex subring of algebraic integers. Since p is not a unit in this ring (since $1/p$ is not an integer; not integral in $\mathbb{Q}$), there must be an E such that p does not divide $(\dim E)\cdot \mathrm{ch}_E(g)$. In particular, p does not divide $\dim E$ and $(\dim E)\cdot \mathrm{ch}_E(g) \neq 0$ so $\mathrm{ch}_E(g) \neq 0$ as desired. ■

We can now prove Burnside's theorem:

Proof (Burnside)

We know that finite p-groups (groups of order p^n) are solvable. So we will show that if G's order is divisible by precisely two primes, then G is not simple. This is sufficient: inducting over the order of the group, a normal subgroup in G is either a p-group (and thus solvable) or has order divisible by precisely two primes (solvable by induction), similar for G/N, and so G is solvable.

So let G be a group whose order is divisible by two primes, p and q. If $Z(G)$ is nontrivial, then G is not simple. Otherwise $Z(G) = 1$, then the sum of the orders of the non-trivial conjugacy classes is not divisible by pq (let $C_1, \ldots, C_n$ be thee non-trivial conjugacy classes, then $|G| \equiv |C_1| + \cdots + |C_n| + 1 \equiv 0 \pmod{pq}$, since pq doesn't divide 1, it doesn't divide the sums of $|C_i|$). Thus there must be a conjugacy class whose order is not divisible by p or q. Since the order of each conjugacy class divides the order of $|G|$, this means such a conjugacy class's order is a positive power of p or q, and the result follows from the previous proposition. ■