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 $[\bullet]_d : \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ 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 $\delta_a : (\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}$ 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

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