GROUPS AND GROUP ACTIONS.

1. Groups

We begin by giving a definition of a group:

Definition 1.1. A group is a quadruple $(G, e, \star, \iota)$ consisting of a set G, an element $e \in G$, a binary operation $\star\colon G \times G \to G$ and a map $\iota\colon G \to G$ such that

(1) The operation $\star$ is associative: $(g \star h) \star k = g \star (h \star k)$,
(2) $e \star g = g \star e = g$, for all $g \in G$.
(3) For every $g \in G$ we have $g \star \iota(g) = \iota(g) \star g = e$.

It is standard to suppress the operation $\star$ and write gh or at most $g.h$ for $g \star h$. The element e is known as the *identity element*. For clarity, we may also write e_G instead of e to emphasize which group we are considering, but may also write 1 for e where this is more conventional (for the group such as $\mathbb{C}^*$ for example). Finally, $\iota(g)$ is usually written as g^{-1}.

Remark 1.2. Let us note a couple of things about the above definition. Firstly *closure* is not an axiom for a group whatever anyone has ever told you[1]. (The reason people get confused about this is related to the notion of subgroups – see Example 1.8 later in this section.) The axioms used here are not "minimal": the exercises give a different set of axioms which assume only the existence of a map ι without specifying it. We leave it to those who like that kind of thing to check that associativity of triple multiplications implies that for any $k \in \mathbb{N}$, bracketing a k-tuple of group elements $(g_1, g_2, \ldots, g_k)$ in any fashion yields the same answer, so that we can write products $g_1 g_2 \ldots g_k$ unambiguously.

Example 1.3. Groups arise naturally when you consider the symmetries of an object. For example, there are six symmetries of an equilateral triangle: the identity[2], the rotations by $2\pi/3$ and $4\pi/3$, and the reflections in the three lines through a vertex and the midpoint of the opposite side. In this case the group is small enough that writing down a table of all the compositions to understand the multiplication is not completely unreasonable (such a table is known as a "Cayley table").

Example 1.4. Some more general examples: for any set X, let $\mathcal{S}_X$ be the set of bijections from X to itself, *i.e.* maps $\alpha\colon X \to X$ which are injective and surjective. The set $\mathcal{S}_X$ is naturally a group, where the group operation $\star$ is given by composition of functions. In the case X is a finite set, these groups are known as *symmetric groups*. Since any two sets with the same number of elements are in bijection, it is easy to see that $\mathcal{S}_X$ is isomorphic to $\mathcal{S}_Y$ if and only if $|X| = |Y|$. Because of this we normally assume that the set X consists of the first n positive integers $\{1, 2, \ldots, n\}$,

---

Date: January 2009.

[1] If you look at Wikipedia (as you should for many things) it gets this wrong. As a general principle, you should use Wikipedia as a resource, but only as a first reference, not as a bible.

[2] the "do nothing" symmetry: if you object to this as a symmetry, you have a point, but only as good a point as the objection to zero as a number, which hopefully you've gotten over.

and write S_n for the symmetric group on a set of n elements. Note that when X is finite, $\alpha\colon X \to X$ is a bijection if and only if it is an injection, if and only if it is a surjection.

We've sneaked in the notion of an isomorphism of groups, which was cheating, so you're owed another definition.

Definition 1.5. Let G and H be groups. A map $\alpha\colon G \to H$ is said to be a homomorphism if it preserves the group operation, that is, if

$$\alpha(g.h) = \alpha(g).\alpha(h), \quad \forall g, h \in G.$$

If there is a homomorphism $\beta\colon H \to G$ such that $\beta \circ \alpha = \mathrm{id}_G$, and $\alpha \circ \beta = \mathrm{id}_H$ then we say that α is an isomorphism.

Example 1.6. The integers $\mathbb{Z}$ form a group under addition, where the identity element is 0. Given a positive integer n, the integers modulo n form a group $\mathbb{Z}/n\mathbb{Z}$ under addition. These are the cyclic groups. Any group generated by a single element is isomorphic to one of these groups.

Example 1.7. Let V be a finite dimensional vector space over a field k (*e.g.* the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$). Then the set of all invertible linear maps from V to itself forms a group under composition, known as the automorphisms of V or the *general linear group* $\mathrm{GL}(V)$.

$$\begin{aligned}\mathrm{GL}(V) &= \{\alpha\colon V \to V : \alpha \text{ linear and invertible}\}\\ &= \{\alpha\colon V \to V : \alpha \text{ linear and injective}\}\\ &= \{\alpha\colon V \to V : \alpha \text{ linear and surjective}\}.\end{aligned}$$

where the last two equalities hold because $\dim(V) = \dim(\mathrm{im}(\alpha)) + \dim(\mathrm{ker}(\alpha))$ (the rank-nullity equation). More concretely, if n is a positive integer, the set

$$\mathrm{GL}_n(\mathsf{k}) = \{A \in \mathrm{Mat}_n(\mathsf{k}) : A \text{ is invertible}\},$$

of invertible $n \times n$ matrices over k is a group. Since a matrix is invertible if and only if its determinant is nonzero, we may also describe this group as

$$\mathrm{GL}_n(\mathsf{k}) = \{A \in \mathrm{Mat}_n(\mathsf{k}) : \det(A) \neq 0\}.$$

Picking a basis $\{e_1, e_2, \ldots, e_n\}$ of V, gives an isomorphism $\mathrm{GL}(V) \to \mathrm{GL}_n(\mathsf{k})$ sending $\alpha \in \mathrm{GL}(V)$ to $A = (a_{ij})$ where $\alpha(e_i) = \sum_{i=1}^n a_{ij} e_i$. Much of this course will be concerned with the study of homomorphisms from a finite group G to the groups $\mathrm{GL}(V)$ for V a complex vector space. However the general linear group also gives interesting examples of finite groups when we take k to be a finite field.

Notice that the previous example is an instance of a general phenomenon: Given a vector space V, we could consider $\mathcal{S}_V$ the group of all bijections $V \to V$, as in Example 1.4. It is more natural to consider the subgroup of $\mathcal{S}_X$ consisting of those bijections which are compatible with the linear structure, that is, the general linear group. If V was, say, an $\mathbb{R}$-vector space equipped with a dot product so that we had a notion of distance, then it would make sense to restrict further to the group of distance-preserving linear transformations $\mathrm{O}(V)$ (the *orthogonal group*). The more structure an object has, the more refined its group of symmetries will be.

Example 1.8. If G and H are groups, we can build a new group $G \times H$ in an obvious way. The underlying set is just the Cartesian product $G \times H$, and the operation is "componentwise", that is

$$(g, h).(g', h') = (gg', hh'), \quad \forall g, g' \in G, h, h' \in H.$$

Then it is easy to check the axioms for a group are satisfied. For example, the identity element is (e_G, e_H).

Example 1.9. Another way to find new groups from ones you already have is to find *subgroups*. A subgroup of a group G is a subset H of G containing e such that if $g, h \in H$ then $g.h \in H$ and $g^{-1} \in H$. When this holds it is easy to check that H is a group. (This is where the term *closure* comes from – H is a subgroup of G if it is *closed* under the group operations.) It is straight-forward to show that H is a subgroup of G if and only if H is nonempty and for $g, h \in H$ we have $gh^{-1} \in H$.

It turns out that *every* finite group is a subgroup of some symmetric group, so in some sense this allows you to find all finite groups. However since finding all the subgroups of a given group is a hard task, this turns out to be a less useful observation than it might at first sight seem.

2. Group actions

We want define the notion of a "group action". In many parts of mathematics, if you are studying some object it is useful to understand what symmetries it has. Since symmetries of a space are invertible and closed under composition they naturally have a group structure. In representation theory, one turns this strategy somewhat on its head, and asks, for a given group G, which spaces have G as their group of symmetries[3]. Of course I have been deliberately vague in using the word "space" here: in fact the question is a good (but hard, indeed sometimes essentially hopeless) one for various classes of spaces, such as vector spaces, smooth manifolds, algebraic varieties *etc.*. We shall start by considering one of the simplest possibilities – a set.

Definition 2.1. Let X be a set and G a group. An *action* of G on X is a map $a \colon G \times X \to X$ such that

(1) $a(gh, x) = a(g, a(h, x))$, for all $g, h \in G, x \in X$.
(2) $a(e, x) = x$, for all $x \in X$.

Often the map a is suppressed in the notation, and one writes $g(x)$, or $g \cdot x$ for $a(g, x)$. In this notation the first condition for a group action becomes perhaps more natural looking: $g \cdot (h \cdot x) = (gh) \cdot x$. A set X with an action of a group G is often known as a G-set.

Recall from the previous section that for any set X, the set $\mathcal{S}_X$ of all bijections $\alpha \colon X \to X$ is naturally a group under composition. The following lemma gives another way to think about group actions.

Lemma 2.2. *Let X be a set and G a group. The structure of an action of G on X is equivalent to a giving a homomorphism of groups $\alpha \colon G \to \mathcal{S}_X$.*

[3] In fact one usually asks just for a map from G to the full group of symmetries of the space, as we will see below.

Proof. Suppose a is an action of G on X. Then set $\alpha(g)(x) = a(g, x)$. It is easy to check that $\alpha(g)$ is a bijection, and α is a group homomorphism. Similarly, given $\alpha\colon G \to \mathcal{S}_X$, if we set $a(g, x) = \alpha(g)(x)$ we obtain an action of G on X. □

We shall often abuse notation somewhat, and refer to a homomorphism from G to $\mathcal{S}_X$ as an action, though they are not literally the same thing.

Example 2.3. The symmetric group S_n acts on $\{1, 2, \dots, n\}$ in the obvious way (with the associated homomorphism α being the identity map).

Example 2.4. Let G be the symmetries of the equilateral triangle. Then G acts on the set of vertices of the triangle.

Example 2.5. Given a G-set X we can build new G-sets from it in various natural ways. For example, let $\mathcal{P}(X)$ be the *power set* of X, that is, the set of all subsets of X. Clearly an action of G on X induces an action of G on $\mathcal{P}(X)$. Indeed this can be refined a little: if $k \in \mathbb{N}$ is a positive integer and $\mathcal{P}_k(X)$ denotes the set of subsets of X which have k elements, then the action of G on $\mathcal{P}(X)$ restricts to give an action on $\mathcal{P}_k(X)$.

Example 2.6. In a similar vein, if X and Y are G-sets, then their disjoint union $X \sqcup Y$ is a G-set where G acts in the obvious way. Somewhat more subtly, the Cartesian product $X \times Y$ is naturally a G-set with the action $g \cdot (x, y) = (g \cdot x, g \cdot y)$ for $x \in X, y \in Y, g \in G$.

Example 2.7. Any group G acts on itself by "left multiplication": simply take the map $a\colon G \times G \to G$ to be the multiplication in G, that is, the associated homomorphism $\lambda\colon G \to \mathcal{S}_G$ is given by $\lambda(g)(h) = g.h$, $(g, h \in G)$. We can also use "right multiplication", but in that case the homomorphism $\rho\colon G \to \mathcal{S}_G$ must be $\rho(g)(h) = hg^{-1}$ (check you see the reason for the inverse). We will use the left (or right) action combined with the power set construction later to prove the famous Sylow theorem.

Example 2.8. An easy but useful observation about the previous two actions is that they commute:

$$\lambda(g)\rho(h)(x) = \rho(h)\lambda(g)(x) = gxh^{-1}, \quad \forall g, h, x \in G.$$

so that in fact we have an action of $G \times G$ on G. Using the fact that we can embed any group G into $G \times G$ "diagonally" via the map $\Delta\colon G \to G \times G$, $\Delta(g) = (g, g)$, this gives us yet another action of G on itself, the *conjugation* or *adjoint* action of G. We will write this as $c\colon G \to \mathcal{S}_G$, so that

$$c(g)(x) = gxg^{-1}.$$

This action of G has a property not satisfied by the left and right actions that we already considered – it respects the group operation:

$$c(g)(x.y) = c(g)(x).c(g)(y) \quad \forall x, y, g \in G,$$

since $c(g)(x).c(g)(y) = (gxg^{-1}).(gyg^{-1}) = g(xy)g^{-1} = c(g)(xy)$. Therefore $c(g)$ is not just a bijection from the set G to itself, it is a homomorphism (and thus an isomorphism). The set of isomorphisms from G to itself is a subgroup of $\mathcal{S}_G$ denoted Aut(G). Thus we see that c is a homomorphism

$$c\colon G \to \text{Aut}(G).$$

The fundamental question on group actions is to classify, for a given group G, all possible sets with a G-action. The first step, as always with such classification problems, is to decide when we wish two consider to G-sets equivalent.

Definition 2.9. Let X and Y be G-sets. A map $f\colon X \to Y$ is said to be *G-equivariant* if

$$f(g \cdot x) = g \cdot f(x), \quad \text{for all } x \in X, g \in G.$$

In terms of the associated homomorphisms $\alpha\colon G \to \mathcal{S}_X$ and $\beta\colon G \to \mathcal{S}_Y$ we can write this condition as follows: for each $g \in G$ the square

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\alpha(g)"'] & Y \arrow[d, "\beta(g)"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

commutes. We say that two G-sets X and Y are *isomorphic* if there is a G-equivariant bijection $f\colon X \to Y$.

Thus the more precise version of our classification problem is to classify G-sets up to isomorphism. We now make the initial steps towards an answer to this problem.

Definition 2.10. Given a set X with an action of a group G, there are some naturally associated subgroups of G and subsets of X which we now want to consider. Let x_0 be a point of X. The *G-orbit* of x_0 is the set

$$G(x_0) = \{g \cdot x_0 \in X : g \in G\}.$$

It consists of the *translates* of x_0 by the elements of G. The *stabilizer* of x_0 is the set

$$G_{x_0} = \{g \in G : g \cdot x_0 = x_0\}.$$

Note that $G(x_0) \subset X$ while $G_{x_0} \subset G$. It is easy to see that G_{x_0} is a subgroup of G (check this!)

Lemma 2.11. *Let X be a G-set. Then X is the disjoint union of its G-orbits.*

Proof. Clearly any element of X lies in some orbit, so we only need to show that distinct orbits have no elements in common. Suppose $G(x_0)$ and $G(x_1)$ are two orbits which are not disjoint, so that for some $y \in X$ we have $y \in G(x_0) \cap G(x_1)$. We must show that in fact $G(x_0) = G(x_1)$. But by definition we have $y = g_0 \cdot x_0$ and $y = g_1 \cdot x_1$ for some $g_0, g_1 \in G$, and so setting $g = g_1^{-1}g_0$ we find $g \cdot x_0 = x_1$. Therefore if $z \in G(x_1)$ so that $z = h \cdot x_1$, we have

$$z = h \cdot x_1 = h \cdot (g \cdot x_0) = (hg) \cdot x_0,$$

and so $z \in G(x_0)$. Thus we see that $G(x_1) \subseteq G(x_0)$. On the other hand (using $x_0 = g^{-1}x_1$) the same argument shows that $G(x_0) \subseteq G(x_1)$, and so $G(x_0) = G(x_1)$ as required. □

Lemma 2.11 allows us to reduce our classification problem to the case where X is a single G-orbit. Such G-sets are called *transitive* G-sets, or sometimes *homogeneous* G-sets.

Example 2.12. If $X = \{1, 2, \dots, n\}$ and $\sigma \in S_n$ any element of the symmetric group, then the cyclic group $G = \{\sigma^n : n \in \mathbb{Z}\}$ generated by σ acts on X (where the associated homomorphism α is just the inclusion map). The set X is therefore the disjoint union of its G-orbits, each of which have a simple form. Indeed let $r \in X$. The orbit $\mathcal{O}$ of r is just $\{\sigma^i(r) : i \in \mathbb{Z}\}$. Since $\mathcal{O} \subset X$, clearly not all of $r, \sigma(r), \sigma^2(r), \ldots, \sigma^n(r)$ can be distinct, and moreover if $\sigma^i(r) = \sigma^j(r)$ for $i < j$ then $r = \sigma^{j-i}(r)$. It follows that the orbit is just the set $\{r, \sigma(r), \ldots, \sigma^{i-1}(r)\}$, where i is the smallest positive integer with $\sigma^i(r) = r$.

Consider as an explicit example S_5 and the element $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$, where σ sends the number i in the top row to the number beneath it in the second row. Then the orbits are:

$$\begin{tikzcd} 1 \arrow[r] & 3, \arrow[dl] & & 4 \arrow[r, leftrightarrow] & 5. \\ 2 \arrow[u] & & & & \end{tikzcd}$$

This allows us to represent σ in the more compact *cycle notation*: we represent each orbit as a sequence $(r_1, r_2, \ldots, r_k)$ so that $\sigma(r_i) = r_{i+1}$ if $i < k$ and $\sigma(r_k) = r_1$, by arbitrarily picking a member of the orbit to start the sequence. Thus we can write σ above as $(132)(45)$ (by picking other elements to start the sequences we could also represent σ as $(213)(54)$ or $(321)(45)$ *etc.*).

Example 2.13. The orbits of the action of G on itself via the conjugation action c are known as *conjugacy classes*. It is easy to see that the kernel of the map $c \colon G \to \mathrm{Aut}(G)$ is exactly the centre of G, denoted $Z(G)$, since $c(g)$ is the identity if and only if $c(g)(x) = x$ for all $x \in G$, which is to say

$$gxg^{-1} = x \iff gx = xg, \quad \forall x \in G.$$

Since the last equation is symmetric in x and g we see that $c(g)(x) = x$ if and only if $c(x)(g) = g$, and so $Z(G)$ can also be characterized as the union of the orbits of size 1 for the conjugation action. It is a useful exercise to check that the conjugacy classes of the symmetric group S_n are given by the cycle type: that is by the sizes of the cycles the permutation decomposes $\{1, 2, \ldots, n\}$ into.

Example 2.14. Most of what we have said here is also interesting for groups which are not finite. Let $G = \mathrm{SO}_3(\mathbb{R})$ be the group of orientation preserving linear isometries of $\mathbb{R}^3$. Then G acts on $\mathbb{R}^3$ in the obvious way, and the orbits of the action are just spheres centered at the origin (including the origin itself as the sphere of radius 0). Thus $\mathbb{R}^3$ is the disjoint union of its G-orbits. Since there are infinitely many orbits, this does not translate into a simple counting formula, but it is a phenomenon you probably used when evaluating integrals in polar coordinates.

3. Classification of G-sets and applications of Group Actions

Consider two point x, y of some G-set X. We would like to know how their stabilizers are related. If x and y belong to different orbits there is no *a priori* relationship between their stabilizers, but on the other hand if x and y do lie in the same G-orbit, then we can say precisely what the relationship is.

Lemma 3.1. *Let X be a G-set, and suppose that $x, y \in X$ lie in the same orbit. Then if $g \in G$ is such that $y = g(x)$ we have*

$$gG_xg^{-1} = G_y.$$

Moreover, if we set $G_{x,y} = \{h \in G : h(x) = y\}$ *then we have*

$$G_{x,y} = gG_x = G_y g.$$

Proof. Suppose that $h \in G_x$, so $h(x) = x$. Then we see that

$$(ghg^{-1})(y) = g(h(g^{-1}(y))) = g(h(x)) = g(x) = y$$

and so ghg^{-1} belongs to G_y. Hence we see that

$$gG_xg^{-1} = \{ghg^{-1} | h \in G_x\} \subseteq G_y.$$

But now we have shown this for arbitrary $x, y \in X, g \in G$, so we may replace them by y, x, and g^{-1} respectively to obtain

$$g^{-1}G_yg \subseteq G_x \iff \quad G_y \subseteq gG_xg^{-1}.$$

Combining these two inclusions we see that $G_y = gG_xg^{-1}$ as required.

To see the last part, note that if $k \in G_x$ then clearly $(gk)(x) = g(k(x)) = g(x) = y$, so that $gG_x \subseteq G_{x,y}$. Conversely, if $h(x) = y$, the clearly $g^{-1}h \in G_x$, so that $G_{x,y} \subseteq gG_x$. □

Remark 3.2. In general, given a group G and two arbitrary subgroups H and K, we say that H and K are *conjugate* if there is a $g \in G$ such that $H = gKg^{-1}$, that is if $c(g)(H) = K$. This gives an equivalence relation on the set of subgroups of G.

For a subgroup H of G we call the subsets of G of the form gH the *left cosets* of H and those of the form Hg the *right cosets* of H. They can be characterized as the orbits of the action of H on G via right or left multiplication respectively.[4]

In a fit of pedagogical opportunism, let's also quickly recall the notion of a quotient group. Suppose that N is a subgroup of G, and G/N its left cosets. We wish to study when the multiplication on G induces a group structure on the set G/N. If gN and hN are two N-cosets then the set

$$gN.hN = \{gn_1hn_2 : n_1, n_2 \in N\}$$

is clearly stable under right multiplication by N, so that it is a union of left N-cosets, which (taking $n_1 = e$) includes the coset $(gh)N$. Thus in order for this to allow us to define a group structure on G/N we must have $gN.hN = (gh)N$ for all $g, h \in G$.

Suppose that this condition holds. Then taking $h = g^{-1}$ we see that $gng^{-1} \in gN.g^{-1}N = (gg^{-1})N = N$. Thus $c(g)(N) = N$ for all $g \in G$. On the other hand, suppose that $c(g)(N) = N$ for all $g \in G$. Then

$$gn_1hn_2 = (gh)(h^{-1}n_1k)n_2 = (gh)c(h^{-1})(n_1)n_2 \in (gh)N.$$

so that $gN.hN = (gh)N$.

If N is a subgroup such that $c(g)(N) = N$ for all $g \in G$, then we say that N is a *normal subgroup*[5] of G. When N is normal, we have just shown that G/N has a binary operation given by $gN.hN = (gh)N$, and it is easy to check that G/N then inherits a group structure from G.

---

[4]Perversely, the orbits for the *right* action of H on G are the *left cosets* and correspondingly the orbits for the left action are the right cosets. Not my fault.

[5]Thus a subgroup is normal if and only if it is a union of conjugacy classes.

Now suppose that X is an arbitrary G-set and $\mathcal{O}$ an orbit in X. Pick a point $x \in \mathcal{O}$ and then for each $y \in \mathcal{O}$, pick $g_y \in G$ such that $g_y(x) = y$. Clearly we have

$$\mathcal{O} = G(x) = \{g_y \cdot x : y \in \mathcal{O}\},$$

Since every element of G maps x to one of the $g_y \cdot x$ it follows from Lemma 3.1 that

$$G = \bigcup_{y \in \mathcal{O}} g_y G_x. \tag{3.1}$$

Moreover the sets on the right-hand side are evidently pairwise disjoint. This shows that the group G is partitioned by its left cosets with respect to G_x.

A simple consequence of this when G is finite is the *orbit-stabilizer theorem*.

Lemma 3.3. *Suppose that G is a finite group and X is a G-set. For any $x \in X$ we have:*

$$|G| = |G_x|.|G(x)|. \tag{3.2}$$

Proof. In the notation of the previous paragraph, we have already established that G is the disjoint union of G_x-cosets: $G = \bigcup_{y \in G(x)} g_y G_x$, and so

$$|G| = \sum_{y \in G(x)} |g_y G_x|.$$

Now observe that for any $k \in G$ the map $\lambda_k \colon G \to G$ given by $\lambda_k(g) = kg$ is a bijection from G_x to kG_x and so the cosets all have $|G_x|$ elements, and we are done. $\square$

Suppose that X is a transitive G-set. Pick $x_0 \in X$ and let G_{x_0} be its stabilizer. As we have just seen, for any $x \in X$ the set of $g \in G$ which map x_0 to x is a coset of G_{x_0}, so the map $\tilde{b} \colon G \to X$ which sends $g \mapsto g \cdot x_0$ induces a bijection $b \colon G/G_{x_0} \to X$ between X and the cosets of G_{x_0}. Now G/G_{x_0} is naturally a G-set since we can make G act on G/G_{x_0} by setting $g \cdot (kG_{x_0}) := (gk)G_{x_0}$. The map b is then in fact G-equivariant, since

$$b(g \cdot kG_{x_0}) = b((gk)G_{x_0}) = (gk) \cdot x_0 = g \cdot (k \cdot x_0) = g \cdot b(kG_{x_0}),$$

hence the G-sets G/G_{x_0} and X are isomorphic.

The construction of a G-action on the set of cosets G/G_{x_0} clearly makes sense for any subgroup H of G, and the G-set we get in this way is evidently transitive. Thus associating to a subgroup H of G the G-set G/H gives us a map from subgroups of G to transitive G-sets. Moreover, up to isomorphism every transitive G-set arises in this way, as we have just shown that any transitive G-set X is isomorphic to G/G_x for any $x \in X$.

Note that the stabilizer of $eH \in G/H$ is H, since $gH = H$ if and only if $g \in H$. Indeed if $g \in H$, then since H is a subgroup clearly $gH = H$, and conversely if $gH = H$, then $g = g.e \in gH = H$. If we assume that G is a finite group, then applying the orbit-stabilizer theorem to $eH \in G/H$ this implies that

$$|G| = |H|.(G : H),$$

where $(G : H)$ is the number of cosets of H in G. This last equation is known as *Lagrange's theorem*.

We can now prove a classification theorem for G-sets. For a G-set X we write $[X]$ to denote the isomorphism class of X (that is, the collection of all G-sets isomorphic to X).

Theorem 3.4. *The map $H \mapsto G/H$ induces a bijection*

$$\gamma\colon \{\textit{conjugacy classes of subgroups of } G\} \to \{\textit{transitive } G\textit{-sets}\}/\textit{isomorphism}$$

Thus transitive G-sets are classified by the conjugacy classes of subgroups of G.

Proof. Let $\tilde{\gamma}$ denote the map from subgroups of G to isomorphism classes of G-sets G-sets given by $H \mapsto [G/H]$. We have already seen that $\tilde{\gamma}$ is surjective, so to see that $\tilde{\gamma}$ induces the bijection γ it only remains to check when two subgroups H and K yield isomorphic G-sets.

If X and Y are isomorphic G-sets, then an argument similar to the proof of Lemma 3.1 shows that the stabilizers of points in X and Y are conjugate subgroups of G. Hence if G/H is isomorphic to G/K, then H and K are conjugate subgroups of G. On the other hand, if $K = gHg^{-1}$ for some $g \in G$, so that $gH = Kg$, it is easy to check that $tK \mapsto tKg = tgH$ gives an isomorphism between the G-sets G/H and G/K. Thus G/H and G/K are isomorphic G-sets if and only if H and K are conjugate subgroups. □

Remark 3.5. When we allow X to have more structure (*e.g.* a topology or a metric say) and require that the G-action respect that structure, then the classification of the different G-spaces becomes considerably more subtle. Much of this course will be concerned with the case where X is a complex vector space and G is a finite group acting linearly on X.

Example 3.6. Let $G = D_8$, the group of symmetries of a square. If R denotes the rotation by $\pi/2$ counterclockwise, S_1, S_2 the two reflections about the lines through the midpoints of edges, and T_1, T_2 the reflections about the lines through opposite vertices, then

$$G = \{1, R, R^2, R^3, S_1, S_2, T_1, T_2\}.$$

Using the previous theorem, we can describe all the transitive G-sets of this group up to isomorphism by finding the conjugacy classes of subgroups of G. By Lagrange's theorem, a subgroup H of G can have $1, 2, 4$ or 8 elements, and conjugate subgroups of course have the same number of elements, so we may study classes of subgroups using the order of the subgroup.

If $|H| = 8$, then clearly $H = G$, and similarly if $|H| = 1$ then $H = \{1\}$, so it remains to consider the cases $|H| = 2, 4$. Subgroups of index 2 are in bijection with elements of order 2, so it is easy to see that there are three such subgroups up to conjugacy (*i.e.* three conjugacy classes of elements of order 2) indeed $\{R^2, S_1, T_1\}$ give representatives. If $|H| = 4$, then since index two subgroups are normal (*why*?), it is enough to find all subgroups of order 4. By considering the reflections in H, you can check that the possibilities are:

$$\{1, R, R^2, R^3\}, \quad \{1, S_1, S_2, R^2\}, \quad \{1, T_1, T_2, R^2\}.$$

Let P be a point on the square, and consider its orbit under the action of G. Up to isomorphism, the transitive G-set you obtain is one of three possibilities – the stabilizer of P will be trivial or an order two subgroup containing a reflection. Can you find explicit realizations of the other transitive G-sets?

We end this section by giving an some applications of group actions to the study of finite groups. There are a number of ways in which we can make G act on itself. We have already seen one of these: the *left action* which is given by the map

$a(g,x) = g.x$ (where we denote the corresponding homomorphism by $\lambda\colon G \to \mathcal{S}_G$). This gives a proof of Cayley's embedding theorem which we eluded to earlier. Recall that S_n is the symmetric group on n letters – that is, all bijections of the set $\{1,2,\dots,n\}$ to itself.

Theorem 3.7 (Cayley's Theorem)**.** *Let G be a finite group. Then G is isomorphic to a subgroup of a symmetric group S_n.*

Proof. Let $n = |G|$ the order of G. Then we may choose a bijection between G and $\{1,2,\dots,n\}$, so that we get an identification of $\mathcal{S}_G$ with S_n. The map $\lambda\colon G \to \mathcal{S}_G$ is a group homomorphism, and using the identification of $\mathcal{S}_G$ with S_n we get a homomorphism from G to S_n. Thus it is enough to check that this homomorphism is injective, that is, to check that λ is injective. But since $\lambda(g)(e) = g$ for every $g \in G$, we see that $\lambda(g)$ determines g, hence λ is one-to-one as required. $\square$

Remark 3.8. An obvious practical deficiency of the previous proof is that it embeds a finite group G into a rather huge symmetric group. Indeed if $|G| = n$, then it embeds G into S_n, which is a group of size $n!$. Even for $n = 6$ this is an embedding into S_6, a group of order 720 and in general by Stirling's formula $n! \geq (n/e)^n$.

We can similarly define an action of G using multiplication on the right, rather than the left: let $\rho\colon G \to \mathcal{S}_G$ be given by $\rho(g)(h) = hg^{-1}$. Then it is easy to check that ρ is a homomorphism, and hence defines an action of G on itself. (*Check you understand why there needs to be an inverse in the formula defining ρ.*) One can just as well prove Cayley's theorem using the right action instead of the left action.

As another application of group actions, we prove what is called the first Sylow theorem. Suppose G is a finite group, and let $n = |G|$. For a prime p, we may write $n = p^a r$ where $a \geq 0$ is a nonnegative integer, and r is a positive integer relatively prime to p. For this we need to use a simple lemma on binomial coefficients:

Lemma 3.9. *Let n be positive integer. Suppose that p is a prime and $s \geq 0$ is such that $p^s | n$, but p^{s+1} does not divide n. Then $\binom{n}{p^s}$ is not divisible by p.*

Proof. We have
$$\binom{n}{p^s} = \frac{n(n-1)\dots(n-p^s+1)}{p^s(p^s-1)\dots 1}$$
Let $0 \leq k \leq p^s - 1$. The highest power of p dividing $n-k$, say p^b, is clearly less than p^s, so that $p^b | k$. But then p^b also divides $p^s - k$, so the product as a whole cannot be divisible by p as claimed. $\square$

Theorem 3.10 (Sylow's theorem)**.** *Suppose that G is a finite group of order n and $n = p^a r$ as above. Then G has a subgroup of order p^a.*

Proof. We may assume that $a > 0$. Consider the set $\mathcal{P}$ of subsets of G which have size p^a. The group G acts on this set in the natural way. Let $X \in \mathcal{P}$ and consider the stabilizer of X in G, the subgroup G_X. Considering the action of G_X on G by left multiplication, we see that a subset of G is G_X-stable if and only if it is a union of right cosets of G_X. Hence since by definition G_X stabilizes X, it follows that X is a union of right cosets of G_X, and thus $|G_X|$ is a power of p dividing p^a (the size of X).

Using the orbit-stabilizer theorem for the action of G on $\mathcal{P}$ this shows that if $|G_X| = p^s$ for $s < a$ then the orbit of X in $\mathcal{P}$ will have size divisible by p^{a-s}, a positive power of p. But we have seen in the previous lemma that $|\mathcal{P}|$ is not divisible by p, hence there must be some orbit whose size is also not divisible by p. But then we see that the stabilizer of any element of such an orbit is a subgroup of size p^a, and we are done. □

4. Counting

We now derive a simple formula for the number of orbits of G on X. We will then use it to show that there are very few finite subgroups of the group $\mathrm{SO}_3(\mathbb{R})$. For $g \in G$ let $F_g = |\{x \in X : \rho(g)(x) = x\}$.

Theorem 4.1 (Burnside's lemma[6]). *Let X be a finite set, and let G be a finite group acting on X. Then the number of orbits in X is*

$$|G|^{-1} \sum_{g \in G} |F_g|.$$

Proof. First note the trivial fact that $\sum_{x \in E} 1 = |E|$ for any finite set E. Now consider the finite set

$$Z = \{(g.x) : g \in G, x \in X, x \in F_g\} = \{(g,x) : g \in G, x \in X, g \in G_x\}.$$

Then by counting the elements of Z in the two ways suggested by the two descriptions we see that

$$\sum_{g \in G}(\sum_{x \in G_x} 1) = \sum_{x \in X}(\sum_{g \in G_x} 1).$$

Now suppose that X is a union of the orbits $\mathcal{O}_1, \mathcal{O}_2, \dots \mathcal{O}_r$. Then we see that

$$\sum_{g \in G} |F_g| = \sum_{x \in X} |G_x| = \sum_{j=1}^{r}(\sum_{x \in \mathcal{O}_j} |G_x|).$$

Now the stabilizers of elements in the same orbit are conjugate, and have the same number of elements, namely $|G|/|\mathcal{O}_j|$. Hence the inner sum in the last expression above is just $|G|$. Hence

$$\sum_{g \in G} |F_g| = |G|.r$$

which immediately yields the formula in the statement of the theorem. □

Now suppose that we have a finite group G of rotations in $\mathbb{R}^3$ (thus the elements of G are rotations about some axis passing through the origin, by an angle which is a rational multiple of 2π. We will show that are very few such groups. Notice that if G is such a group then G preserves the unit sphere S in $\mathbb{R}^3$.

For each $g \in G$ let $F_g = \{v \in S : g(v) = v\}$, and let $F = \bigcup_{g \in G, g \neq I} F_g$. Notice that for $g \neq I$ the set F_g consists of exactly two antipodal points, so that F is a finite set. Moreover G clearly acts on F. Now if r is the number of G-orbits in F, Burnside's lemma shows that

$$r = \frac{1}{|G|} \sum_{g \in G} |F_g|.$$

[6] This turns out not to be due to Burnside, but rather maybe Cauchy or Frobenius, thus this lemma is also sometimes referred to as "not Burnside's lemma".

Examining the right-hand side, we see that if $g = I$ then $F_g = F$, whereas if $g \neq I$ as noted above we have $|F_g| = 2$. Thus we may rewrite this equation as

$$\begin{aligned} r &= \frac{|F|}{|G|} + \frac{2}{|G|}(|G| - 1) \\ &= \sum_{i=1}^{r} \frac{|\mathcal{O}_j|}{|G|} + \frac{2}{|G|}(|G| - 1), \end{aligned}$$

where $\mathcal{O}_1, \dots \mathcal{O}_r$ are the orbits of G on F. Let n_j be the order of G_x for any $x \in \mathcal{O}_j$ so that by the orbit-stabilizer theorem $n_j|\mathcal{O}_j| = |G|$. Then we may rearrange our equation yet again to find:

$$r = \sum_{j=1}^{r} \frac{1}{n_j} + 2(1 - \frac{1}{|G|}).$$

or equivalently:

$$2 - \frac{2}{|G|} = \sum_{j=1}^{r}(1 - \frac{1}{n_j}). \tag{4.1}$$

Now it turns out that equation (4.1) can be solved. We assume that $|G| \geq 2$, so that we have

$$1 \leq 2 - \frac{2}{|G|} = \sum_{j=1}^{r}(1 - \frac{1}{n_j}) < r.$$

Thus certainly we must have $r \geq 2$. On the other hand, we also have

$$\frac{r}{2} \leq \sum_{j=1}^{r}(1 - \frac{1}{n_j}) = 2 - \frac{2}{|G|} < 2,$$

and so $r < 4$. Hence we see that $r = 2$, or 3. One can analyze these cases to individually to see that the only solutions for the n_j are

- $s = 2$ and $n_1 = n_2 = |G|$.
- $s = 3$ and $(n_1, n_2, n_3, |G|) = (2, 2, n, 2n), (2, 3, 3, 12), (2, 3, 4, 24), (2, 3, 5, 60)$.

It turns out that there is essentially one group corresponding to each of these sets of numbers - they are the finite subgroups of the group of rotations about a fixed axis, the dihedral groups, and the rotational symmetries of the tetrahedron, cube and iscosahedron respectively.

LINEAR REPRESENTATIONS: BASIC THEORY

1. Linear actions

We now get to the main subject of the course: linear representations of groups. Classifying group actions on mathematical objects (differentiable manifolds, algebraic varieties *etc.*) is in general almost hopeless, but as a first approximation one can study linear actions. We are primarily interested in the case of vector spaces over the complex numbers $\mathbb{C}$, but much of what we do works for any algebraically closed field k, with some restrictions on the characteristic (as we will explain later).

Definition 1.1. Let V be a vector space, and $a\colon G \times V \to V$ an action of a group G on the set V. We say that the action is linear if the image of the associated homomorphism $\alpha\colon G \to \mathcal{S}_V$ lies in $\mathrm{GL}(V)$, *i.e.* if the maps $\alpha(g)$ respect the linear structure of V. When we wish to be precise we will write (V, α) for a representation of G, where $\alpha\colon G \to \mathrm{GL}(V)$, but we will often abuse notation somewhat and omit the homomorphism α, writing $g(v)$ or $g \cdot v$ instead of $\alpha(g)(v)$.

If (V, α) is a representation of G, then picking a basis $\{e_1, e_2, \ldots, e_n\}$ of V, we obtain a map $\rho\colon G \to \mathrm{GL}_n$, a *matrix realization* of (V, α). Since the choice of a basis here is often arbitrary, it is often better not to fix one particular such realization, as different computations may be easier with different choices of matrix realizations.

Example 1.2. For any vector space V, the general linear group $\mathrm{GL}(V)$ acts on the vector space V, in the obvious way.

Example 1.3. Let S_n be the symmetric group on n letters. Take an n-dimensional vector space with basis $\{e_1, e_2, \ldots, e_n\}$. Then we may define an action of S_n on W by setting

$$\alpha(g)(e_i) = e_{g(i)},$$

and extending linearly.

Example 1.4. We can generalize the previous example quite easily: suppose that G is a finite group acting on a finite set X. Let $\mathsf{k}[X]$ denote the (k-vector space) of k-valued functions on X. For any $x \in X$ let

$$e_x(y) = \begin{cases} 1, & \text{if } x = y; \\ 0, & \text{otherwise.} \end{cases}$$

It is easy to see that $\{e_x : x \in X\}$ is a basis for $\mathsf{k}[X]$ (indeed to see that it spans[1] $\mathsf{k}[X]$ just note that for any $f \in \mathsf{k}[X]$ we have $f = \sum_{x \in X} f(x) e_x$). Using this basis we may define an action of G by setting

$$g(e_x) = e_{g(x)}, \quad \forall g \in G, x \in X.$$

and extending linearly.

Date: October 28, 2004.

[1]Note that this uses the assumption that X is a finite set.

This action can also be described more intrinsically as follows: given $f \in \mathsf{k}[X]$, let

$$g(f)(x) = f(g^{-1}(x)), \quad \forall g \in G, f \in \mathsf{k}[X], x \in X.$$

This is clearly gives a linear map for each $g \in G$, and

$$(gh)(f)(x) = f((gh)^{-1}x) = f(h^{-1}(g^{-1}(x))),$$

whereas

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

so we have an action (clearly the identity of G acts trivially). It is easy to check that this action coincides with the more explicit one given above.

If $G = S_n$, and $X = \{1, 2, \dots, n\}$, this example reproduces the previous example. Linear representations constructed in this way from G-sets are known as *permutation representations*.

Remark 1.5. Our intrinsic rephrasing is not just for aesthetic purposes. It shows that if G is any group acting on a space X, then we should expect functions on that space to carry a linear representation of G, whether or not G or X is finite. For example suppose that X is a topological space and G acts continuously on X (that is, suppose the map $a\colon G \times X \to X$ is continuous[2]). Then the space $C(X)$ of continuous functions on X becomes a linear representation of X by the above formula.

Example 1.6. Rather less creatively, given any group G, and any vector space V we may define an representation of G on V by letting each $g \in G$ act by the identity. When V is one-dimensional, this is called the *trivial* representation. (The use of the word trivial should be self-explanatory, the motivation for the one-dimensional condition is that we can decompose V into a direct sum of lines, on each of which G also acts trivially, so that V is built as a direct sum from one-dimensional trivial representations of G, so not much is gained by considering other dimensions.)

Example 1.7. Another not terribly imaginative way of producing representations is by direct sum: if (V, ρ) and (W, α) are two linear representations, we can make $V \oplus W$ into a representation of G by letting G act "componentwise". (We will discuss this example in some more detail later.)

Example 1.8. Suppose that $\rho\colon H \to \mathrm{GL}(V)$ is a linear representation of H, and $\phi\colon G \to H$ is a group homomorphism. Then the composition $\rho \circ \phi\colon G \to \mathrm{GL}(V)$ defines a linear representation of G. This is known as the *pull-back* of the representation (V, ρ) by ϕ. Two important cases of this are where G is a subgroup of H (when the pull-back operation is usually called *restriction*) and when H is a quotient of G (in which case the pull-back operation is usually referred to as *lifting*).

The basic problem of representation theory is to classify the representations of a group. Of course, as with our study of group actions, to do this we need to be clear when we consider two representations to be equivalent.

[2]If G is finite, we can just assume that G is a discrete space, but we could also give G a more complicated topology and demand the multiplication *etc.* on G be continuous with respect to it: a group with this extra structure is called a topological group.

Definition 1.9. Let (V, ρ) and (W, σ) be representations of a group G. Then we say that (V, ρ) and (W, σ) are isomorphic if there is a invertible linear map $T\colon V \to W$ such that

$$T(\rho(g)(v)) = \sigma(g)(T(v)), \quad \forall v \in V, g \in G. \tag{1.1}$$

or equivalently so that the diagrams

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "\rho(g)"'] & W \arrow[d, "\sigma(g)"] \\ V \arrow[r, "T"] & V \end{tikzcd}$$

commute for any $g \in G$.Such a linear map is said to be *G-equivariant* or, rather more poetically, an *intertwiner*, and the space of such linear maps is denoted $\mathrm{Hom}_G(V, W)$.

Thus what we actually seek to do is to classify linear representations of a group up to isomorphism. For actions of a group on a finite set, we obtained such a classification theorem in the previous section: any such set is a union of transitive G-sets, and the isomorphism classes of transitive G-sets are in bijection with conjugacy classes of subgroups of G. For linear representations (at least over the complex numbers), we will be able to get a similar, rather deeper, classification.

Before developing some general theory, lets consider some examples we can study just using linear algebra.

Example 1.10. Let $G = \mathbb{Z}$. Then if (V, ρ) is a representation of G, we have $\rho(n) = \rho(1)^n$, so that ρ is completely determined by $\rho(1) \in \mathrm{GL}(V)$. Moreover, for any $T \in \mathrm{GL}(V)$ the map $n \mapsto T^n$ defines a representation of $\mathbb{Z}$. Thus we see that giving an action of G on V is the same as picking an element of $\mathrm{GL}(V)$. Moreover, if T, T' are two such, then they give isomorphic representations if and only if they are conjugate in $\mathrm{GL}(V)$. Hence the isomorphism classes of representations of $\mathbb{Z}$ of dimension n are in bijection with the conjugacy classes of $\mathrm{GL}(V)$. But by the Jordan canonical form, we know how to describe these classes: every class has a representative T which is composed of blocks J_λ where

$$J_\lambda = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$$

Thus we see that a representation of $\mathbb{Z}$ splits up into a direct sum of subrepresentations corresponding to the Jordan blocks. A subrepresentation is simply a subspace of V preserved by all the elements of G.

Note that the subrepresentation corresponding to a single Jordan block itself contains subrepresentations, but it cannot be split apart into a sum of such. Indeed if U is such a subspace and $\{e_1, e_2, \ldots, e_k\}$ is a basis for U with respect to which T is a Jordan block matrix, then the subrepresentations of U are exactly the spaces spanned by $\{e_1\}$, $\{e_1, e_2\}, \ldots, \{e_1, e_2, \ldots, e_{k-1}\}$ and U itself.

A representation is said to be irreducible if it has no nonzero proper subrepresentation. From the above it follows that the only irreducible representations of G are those given by a single Jordan block of size 1 – that is by a one-dimensional representation. Jordan blocks "glue together" irreducible representations in a non-trivial manner. We will see later that this phenomenon cannot happen if G is finite (at least when $\mathrm{char}(\mathsf{k}) = 0$).

Example 1.11. Suppose that $G = S_3$ the symmetries of an equilateral triangle and suppose also $\mathsf{k} = \mathbb{C}$. It is not hard to see that we can present G as:

$$G = \langle s, t : s^2 = t^3 = 1, sts^{-1} = t^{-1} \rangle.$$

by, say, taking $s = (12)$ and $t = (123)$. (In terms of the equilateral triangle, these are reflection about a line through a vertex and the midpoint of the opposite side, and a rotation by $2\pi/3$.) Thus to give a homomorphism of G to $\mathrm{GL}(V)$, is equivalent to giving a pair of linear maps (S, T) such that $S^2 = T^3 = 1$ and $STS^{-1} = T^{-1}$, and two such pairs (S_1, T_1), (S_2, T_2) yield isomorphic representations if we can conjugation one to the other, *i.e.* if we can find R such that $RS_1R^{-1} = S_2$ and $RT_1R^{-1} = T_2$.

If (S, T) is such a pair, $T^3 = 1$ implies that T satisfies a polynomial with distinct roots, and so it must be diagonalizable[3], with eigenvalues $1, \omega, \omega^2$, where $\omega = e^{2\pi/3}$ (so that $\omega^2 = \omega^{-1}$). Let V_λ be the eigenspace of T with eigenvalue λ, so that

$$V = V_1 \oplus V_\omega \oplus V_{\omega^2}.$$

Since $STS^{-1} = T^{-1}$ the map S gives an isomorphism from V_λ to $V_{\lambda^{-1}}$. To see this, suppose that $v \in V_\lambda$. Then we have

$$T^{-1}(S(v)) = S(T(v)) = S(\lambda(v)) = \lambda S(v),$$

that is, $T(S(v)) = \lambda^{-1}S(v)$, so that $S\colon V_\lambda \to V_{\lambda^{-1}}$. To see that S gives an isomorphism, note that the same argument shows that S maps $V_{\lambda^{-1}}$ to V_λ. It follows that S preserves V_1, and gives an isomorphism $V_\omega \to V_{\omega^2}$ which is its own inverse (as $S^2 = \mathrm{id}$.)

Pick a basis $\{e_1, e_2, \dots e_k\}$ of V_ω and set $f_i = S(e_i)$. Then $\{f_1, f_2, \dots, f_k\}$ is a basis of V_{ω^2}. Moreover, letting $W_i = \mathrm{span}(e_i, f_i)$, we see that W_i is a subrepresentation of V (as $S^2 = 1$, so $S(f_i) = e_i$). Next on V_1 we have $S^2 = 1$ also, so that V_1 decomposes into a direct sum $U_1 \oplus U_{-1}$ of eigenspaces for S. Thus we have decomposed V as follows:

$$V = U_1 \oplus U_{-1} \oplus \bigoplus_{i=1}^{k} W_i.$$

Picking bases of U_1 and U_{-1} we can decompose these further into lines each of which is a subrepresentation (since S and T both act as scalars on $U_{\pm 1}$).

Examining what we have found, we see that G has three irreducible representations: the trivial representation, where both S and T are the identity map; the one dimensional representation where T acts by 1 and S acts by -1; and the two-dimensional representation given by any W_i. With respect to the basis $\{e_i, f_i\}$ the matrices for S and T are:

$$T = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

[3]See next section.

Moreover we have shown that any representation of G is a direct sum of these some number of these irreducibles. This phenomenon will turn out to be true for any finite group (at least over the complex numbers).

2. Review of Linear algebra

In this section we review some constructions in linear algebra, which will allow us to build new representations from ones we already know. We will work over an arbitrary field k. We first recall the definition of a direct sum of vector spaces (which was already used in the case of two vector spaces above).

Definition 2.1. Let V be a vector space, and $U_1, U_2, \dots, U_r$ subspaces of V. We say that V is the *internal direct sum* of the subspaces U_i, $(1 \leq i \leq r)$ if every $v \in V$ can be written uniquely as

$$v = u_1 + u_2 + \dots u_r,$$

where $u_i \in U_i$. Note in particular if $r = 2$, then $V = U_1 \oplus U_2$ if and only if $V = U_1 + U_2$ and $U_1 \cap U_2 = \{0\}$.

If V_i $(1 \leq i \leq s)$ are vector spaces then the *external direct sum* of the V_i, denote $V_1 \oplus V_2 \oplus \dots \oplus V_r$ is the vector space of r-tuples $(v_1, v_2, \dots, v_r)$ where $v_i \in V_i$, with addition given componentwise, and scalar multiplication is given by

$$\lambda(v_1, v_2, \dots, v_r) = (\lambda v_1, \lambda v_2, \dots, \lambda v_r).$$

The difference between internal and external direct sums is not something to get worked up about: if V is the internal direct sum of subspaces $U_1, U_2, \dots, U_r$ then there is clearly a canonical isomorphism from the external direct sum of the U_is to V. Indeed this could also be used as a definition of the internal direct sum: V is the internal direct sum of the subspaces $U_1, U_2, \dots, U_r$ if and only if the map $(u_1, u_2, \dots, u_r) \mapsto u_1 + u_2 + \dots + u_r$ from the external direct sum of the U_is to V is an isomorphism.

Given any subspaces $\{U_i : i \in I\}$ of a vector space V, we may also define $\sum_{i \in I} U_i$ to be the intersection of all subspaces of V which contain each of the subspaces U_i. More concretely, it is straighforward to show that $\sum_{i \in I} U_i$ is the subspace of vectors of the form

$$u_{i_1} + u_{i_2} + \dots + u_{i_r},$$

where each $u_{i_j} \in U_{i_j}$, and $i_1, i_2, \dots, i_r \in I$.

Definition 2.2. Suppose that V is a vector space, and that W is a subspace of V. Then since W is subgroup of the abelian group V, we may consider the quotient group V/W. Since the action of the field k preserves W, it is easy to see that V/W also has the structure of a k-vector space. It is called the *quotient vector space*, and the natural quotient map $\pi \colon V \to V/W$ of abelian groups is a linear map.

Lemma 2.3. *Let V be a vector space and W a subspace. Then*

(1) *If V is finite dimensional then*

$$\dim(V) = \dim(W) + \dim(V/W).$$

(2) *If $V = W \oplus U$ for some subspace U, the U and V/W are isomorphic.*
(3) *Suppose V' is another k-vector space, and $W' < V'$. If $\alpha \colon V \to V'$ is a linear map such that $\alpha(W) \subseteq W'$, then α induces a well-defined map $\tilde{\alpha} \colon V/W \to V'/W'$.*

Proof. For the first part, pick a basis $\{e_1, e_2, \ldots, e_k\}$ of W and extend it to a basis $\{e_1, e_2, \ldots, e_n\}$ of V. Then it is easy to see that $\{e_r + W : k+1 \leq r \leq n\}$ is a basis of V/W.

For the last part, suppose that $e+W \in V/W$. Then we set $\tilde{\alpha}(e+W) = \alpha(e)+W'$. To see this is well-defined, note that if e' is another choice of representative for $e+W$, that is $e'+W = e+W$, then $e-e' \in W$, so that $\alpha(e-e') \in W'$. But then $\alpha(e) - \alpha(e') \in W'$ by the linearity of α, so that $\alpha(e) + W' = \alpha(e') + W'$. □

Another basic construction on vector spaces is to take the dual space.

Definition 2.4. For V a k-vector space as before, we let $V^* = \mathrm{Hom}(V, \mathsf{k})$ be the set of linear maps from V to the field k. It is naturally a vector space, known as the *dual space*. For a subspace W of V, we can naturally attach a subspace of V^*: let

$$W^\circ = \{f \in V^* : f(w) = 0, \forall w \in W\}$$

W° is called the *annihilator* of W.

The basic properties of V^* are contained in the following lemma.

Lemma 2.5. *Suppose that V is a vector space and W is subspace. Then we have*

(1) *If V is finite dimensional, then*
$$\dim(W) + \dim(W^\circ) = \dim(V).$$
In particular, taking $W = 0$ we see $\dim(V^*) = \dim(V)$.

(2) *If $\alpha \colon V \to X$ is a linear map, then α induces a natural map $\alpha^t \colon X^* \to V^*$ by*
$$\alpha^t(f)(v) = f(\alpha(v)), \quad \forall f \in X^*, v \in V.$$
The map α^t is called the transpose of α.

(3) *Let $V^{**} = (V^*)^*$ be the dual of V^*. There is a natural map $d \colon V \to V^{**}$ which is an isomorphism if V is finite dimensional.*

Proof. Let $\{e_1, e_2, \ldots, e_k\}$ be a basis of W and extend it to a basis $\{e_1, \ldots, e_n\}$ of V. Define $e_i^* \in V^*$ by setting $e_i^*(e_j) = 1$ if $i = j$ and 0 otherwise, and extending linearly (that this gives a well-defined linear map is exactly the condition that $\{e_1, e_2, \ldots, e_n\}$ is a basis of V). Then it is easy to check that $\{e_1^*, e_2^*, \ldots e_n^*\}$ is a basis of V^* (known as the *dual basis* of V^*) and $\{e_{k+1}^*, \ldots e_n^*\}$ is a basis of W°, proving part (1).

For the second part, one only needs to check that α^t is linear, but this is clear from the definition.

Finally, for the third part let $d \colon V \to V^{**}$ be the map given by

$$d(v)(f) = f(v), \quad \forall f \in V^*.$$

This is clearly linear. Moreover, it is also injective[4]: indeed if $v \in V$ is nonzero, we may find a basis for V which contains v, and the dual basis to this basis then by definition contains an element $f \in V^*$ such that $d(v)(f) = f(v) = 1$, and hence $d(v) \neq 0$. When V is finite dimensional by the first part of $\dim(V^*) = \dim(V)$ so that d is an isomorphism if and only if it is injective. □

[4]The argument proving injectivity goes through even if V is not finite dimensional

Note that if $\alpha\colon V_1 \to V_2$ and $\beta\colon V_2 \to V_3$, then $(\beta \circ \alpha)^t = \alpha^t \circ \beta^t$, so that $(-)^*$ reverses the order of compositions.

These constructions are useful to us because they behave well with respect to linear actions of groups.

Definition 2.6. Let (V, ρ) be a representation of G. We say that a subspace W of V is a *subrepresentation* (or *invariant subspace*) of V if $\rho(g)(W) \subset W$ for all $g \in G$. When this holds, it follows immediately that $\rho(g)_{|W} \in \mathrm{GL}(W)$, so that $(W, \rho_{|W})$ is a linear representation of G. The representation V is said to be *irreducible* if $\{0\}$ is the only proper subrepresentation of V. (Thus we do not consider $\{0\}$ to be an irreducible representation[5]).

Given a representation of a group V and subrepresentations $W_1, W_2, \ldots, W_r$, we say that V is the direct sum of the subrepresentations $\{W_i\}_{1 \leq i \leq r}$ if this is true at the level of vector spaces. Clearly given representations $\{V_i\}_{1 \leq i \leq s}$ we can make the external direct sum $V_1 \oplus V_2 \oplus \ldots \oplus V_r$ into a representation by letting G act diagonally:

$$g(v_1, v_2, \ldots, v_r) = (g(v_1), g(v_2), \ldots, g(v_r)).$$

For any representation V with a subrepresentation W, we can form the *quotient representation*: simply take the quotient vector space V/W and observe that by part (3) of Lemma 2.3 if W is a subrepresentation then V/W has an induced structure of G-representation. The quotient map $\pi\colon V \to V/W$ is G-equivariant, and if W has a G-invariant complement U, it gives an isomorphism between the representations U and V/W.

Given (V, α) a representation of G, we can also make V^* into a representation in a natural way: define $\alpha^*\colon G \to \mathrm{GL}(V^*)$ by

$$\alpha^*(g)(f) = \alpha(g^{-1})^t(f), \quad f \in V^*, g \in G,$$

where $\alpha(g^{-1})^t$ is the transpose of $\alpha(g^{-1})$ defined in Lemma 2.3. Thus for $v \in V$ we have $\alpha^*(g)(f)(v) = f(\alpha(g^{-1})(v))$.

In fact, the dual space is a special case of a more general construction: if V and W are two representations of G, we can make $\mathrm{Hom}(V, W)$ into a G-representation in a similar manner to how we made G act by conjugation on itself. Indeed G acts on V and on W, then $G \times G$ acts on $\mathrm{Hom}(V, W)$: indeed if $\phi \in \mathrm{Hom}(V, W)$, then if we can define, for $(g, h) \in G \times G$ and $\phi \in \mathrm{Hom}(V, W)$,

$$(g, h)(\phi)(v) = g(\phi(h^{-1}(v))), \quad \forall v \in V.$$

Let $\Delta\colon G \to G \times G$ be the diagonal map $g \mapsto (g, g)$. Using Δ we may pull back the action of $G \times G$ on $\mathrm{Hom}(V, W)$ to G, so that $\mathrm{Hom}(V, W)$ gets the structure of a linear representation of G. The dual space construction above can be recovered by taking W to be the trivial representation. Notice also that it follows immediately from the definitions that $\mathrm{Hom}_G(V, W)$ is just the subspace of $\mathrm{Hom}(V, W)$ on which G acts trivially.

Example 2.7. Let $G = \mathbb{Z}$, and let $V = \mathbb{C}^2$. Then let $\rho\colon \mathbb{Z} \to \mathrm{GL}(V)$ be given by

$$\rho(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

[5] In the same way as 1 is not a prime.

with respect to the standard basis $\{e_1, e_2\}$ of $\mathbb{C}^2$. To calculate what the dual of this representation is, let us take the dual basis to the standard basis $\{e_1, e_2\}$, say δ_1, δ_2 (so that $\delta_i(e_j) = 1$ if $i = j$ and 0 otherwise). Then it is easy to see that the matrix of $\rho^*(n) = \rho(-n)^*$ is given by:

$$\rho^*(n) = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}.$$

It is straight-forward to check that (at least over $\mathbb{C}$) that $\rho(1)$ is conjugate to $\rho(1)$, so that the representations (V, ρ) and (V^*, ρ^*) are isomorphic in this case.

Now let us consider subrepresentations of V. Clearly the vector e_1 is fixed by G, and so spans a one-dimensional subrepresentation L of V (a copy of the trivial representation). The quotient V/L is also the trivial representation, since $\rho(n)(e_2 + L) = e_2 + L$. Since G acts nontrivially on V, we see that L cannot have a complement in V.

Finally, for completeness, we give a proof of the characterization of diagonalizability we used earlier.

Lemma 2.8. *Suppose that $\alpha\colon V \to V$ is a linear map such that $p(\alpha) = 0$ where $p \in \mathsf{k}[t]$ is a polynomial which is a product of distinct linear factors (that is p is of the form $\prod_{i=1}^r (t - \lambda_i)$ with the λ_i all distinct). Then V is the direct sum of the eigenspaces of α, that is, α is diagonalizable.*

Proof. Let $p(t) = \prod_{j=1}^r (t - \lambda_j)$ where the $\lambda_j \in \mathsf{k}$ are distinct, and set

$$q_j = p(t)/(t - \lambda_j).$$

Since $\mathsf{k}[t]$ is a principal ideal domain, and $(t - \lambda_j)$ is irreducible for all j, the ideal generated by the q_j must be all of $\mathsf{k}[t]$. Hence we may find $a_j \in \mathsf{k}[t]$ such that

$$1 = \sum_{j=1}^r a_j(t) q_j(t).$$

Set $\pi_j = a_j(\alpha) q_j(\alpha)$, so that $\mathrm{id}_V = \sum_{j=1}^r \pi_j$. Notice that

$$\pi_j \pi_k = 0$$

since it is a multiple of $p(\alpha)$, and therefore we also have

$$\pi_j = \pi_j \circ \mathrm{id}_V = \sum_{k=1}^r \pi_j \pi_k = \pi_j^2.$$

Thus if we set $V_j = \pi_j(V)$, then V is the sum of the subspaces V_j, since if $v \in V$, then

$$v = \sum_{j=1}^r \pi_j(v),$$

and if $v = \sum_{j=1}^r u_j$, with $u_j \in V_j$, then $\pi_j(v) = \pi_j(u_j) = u_j$, since $\pi_j^2 = \pi_j$ implies π_j is the identity on V_j. It follows $V = \bigoplus_{j=1}^r V_j$. Finally, note that $(\alpha - \lambda_j)$ acts as zero on V_j, since $(\alpha - \lambda_j) \circ \pi_j = a_j(\alpha) p(\alpha) = 0$, thus V_j is an eigenspace of α, and α is diagonalizable as claimed. □

3. Complete reducibility

The first major result in the representation theory of finite groups over $\mathbb{C}$ is Maschke's theorem: every representation of a finite group G over $\mathbb{C}$ is a direct sum of irreducible subrepresentations. Note that we saw above that this is *false* for the infinite group $\mathbb{Z}$. Actually, there is nothing particularly special about the complex numbers here – all that is needed is that the characteristic of the field k that we work over not divide the order of our finite group. The next lemma shows that in order to prove this, it is enough to show that every subrepresentation has a G-invariant complement.

Lemma 3.1. *Let (V, α) be a finite-dimensional representation of a group G. If every subrepresentation W of V has a G-invariant complement, then V is a direct sum of irreducible subrepresentations.*

Proof. We use induction on the dimension of V. If V is irreducible, then we are done. Otherwise, let W be an irreducible subrepresentation of V (which exists, for example by picking the subrepresentation of V of smallest positive dimension). Then W has a G-invariant complement U, and $\dim(U) < \dim(V)$, hence by induction U is a direct sum of irreducibles (*why*?). Thus $V = W \oplus U$ is also a direct sum of irreducibles as required. □

Remark 3.2. In fact the converse of this Lemma is also true, as we will see later.

Thus suppose that G is a finite group, and (V, α) is a linear representation of G with a subrepresentation W. We wish to show that W has a G-invariant complement. The basic idea of the proof is to pick an arbitrary vector space complement, and then average it over the group G to obtain a G-invariant complement. The only problem with this strategy is that we don't have a sensible notion of averaging for subspaces. The solution to this is to notice that we can replace complements of W by certain linear maps: projections from V to W.

Definition 3.3. Let V be a k-vector space and $\pi \colon V \to V$ a linear map. If W is a subspace of V, we say that π is a projection to W if $\pi(V) = W$ and π restricted to W is the identity, *i.e.* for every $w \in W$ we have $\pi(w) = w$. We will denote the restriction of π to a subspace W by $\pi_{|W}$.

The next lemma shows that we have a sensible notion of averaging for projections to the same subspace.

Lemma 3.4. *Let V be a vector space over k, and $\pi \colon V \to V$ a linear map.*

(1) *If π is a projection to W, then $V = W \oplus \ker(\pi)$, and π is completely determined by the pair of complementary subspaces $(im(\pi), ker(\pi))$.*
(2) *If $\pi_1, \pi_2, \dots, \pi_k$ are projections to the same subspace W, and $t_1, t_2, \dots, t_k \in \mathsf{k}$ are such that $\sum_{i=1}^k t_i = 1$, then $\pi = \sum_{i=1}^k t_i \pi_i$ is a projection to W. In particular, if k is invertible in the field k, then the average $\frac{1}{k}\sum_{i=1}^k \pi_i$ is a projection to W.*

Proof. For the first part, since $\pi_{|W}$ is the identity, clearly $W \cap \ker(\pi) = \{0\}$. On the other hand, if $v \in V$, then $v - \pi(v)$ lies in the kernel of π, since $\pi(v - \pi(v)) = \pi(v) - \pi^2(v)$, and $\pi(\pi(v)) = \pi(v)$, since $\pi(v) \in W$ and π is the identity on vectors in W. Thus $V = W \oplus \ker(\pi)$. This also makes it is clear that π is determined by the pair of subspaces $(\mathrm{im}(\pi), \ker(\pi))$.

For the second part, if $w \in W$, then $\pi_j(w) = w$ for each j, and hence clearly $\pi(w) = w$, so that $\pi_{|W}$ is the identity map. On the other hand, the image of $\pi = \sum_{i=1}^k t_i\pi_i$ is clearly contained in W, since this is true for each π_i, so that $\mathrm{im}(\pi) \subseteq W$. It follows that π is a projection to W as claimed. □

Remark 3.5. The lemma shows that the set of projections to a given subspace is an affine subspace in the vector space of all linear maps $\mathrm{End}(V)$ from V to itself, *i.e.* a translate of a linear subspace of $\mathrm{End}(V)$. In the exercises you are asked to compute the dimension of this affine subspace using matrices. The second part of the previous lemma can also be proved using this matrix description.

Let $\mathcal{C}$ be the set of subspaces which are complements to W, let $\mathcal{P}$ be the set of projections to W and let $k\colon \mathcal{P} \to \mathcal{C}$ the map given by taking the kernel, that is $k(\pi) = \ker(\pi)$. Then the first part of the lemma shows that k is a bijection. Now each of the sets $\mathcal{C}$ and $\mathcal{P}$ naturally has a G-action when W is a subrepresentation of V. Indeed if U is a complement to W, then so is $g(U)$ for any $g \in G$, since $g(U)$ has complementary dimension to W, and

$$\{0\} = g(W \cap U) = g(W) \cap g(U) = W \cap g(U).$$

On the other hand, $\mathcal{P}$ is a subset of $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ which is a representation of V via $g(\alpha) = g\alpha g^{-1}$. This action preserves the set $\mathcal{P}$, since if $\pi \in \mathcal{P}$ and $w \in W$, then $g^{-1}(w) \in W$ so that $g\pi g^{-1}(w) = g(g^{-1}(w)) = w$ for $w \in W$, and certainly $g\pi g^{-1}(v) \in W$ for all $v \in V$, since $\pi(V) = W$ and $g(W) = W$.

The map k is a G-equivariant bijection: indeed it's easy to check that $\ker(g\pi g^{-1}) = g(\ker(\pi))$. Thus finding a G-invariant complement to W is equivalent to finding a G-invariant projection from V to W.

Theorem 3.6 (Maschke)**.** *Let G be a finite group, and k a field such that char(k) does not divide $|G|$. Let (V, α) be a representation of G over k, and let W be a subrepresentation of V. Then W has a G-invariant complement.*

Proof. We have shown above that it is enough to produce a G-invariant projection to W. To construct such a projection, first pick an arbitrary projection $\pi\colon V \to W$, and then define

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

We claim that π^G is a G-equivariant projection from V to W. Indeed since we have just checked that G acts on the space of projections to a subrepresentation, each term in the summation is a projection to W, and then by the second part of Lemma 3.4 it follows the average of these projections is again a projection to W.

It remains to check that π^G is G-equivariant. For this it is enough to check that $\alpha(h)\pi^G\alpha(h)^{-1} = \pi^G$ for all $h \in G$. But

$$\begin{aligned}\alpha(h)\pi^G\alpha(h)^{-1} &= \sum_{g \in G} \alpha(h)\alpha(g)\pi\alpha(g^{-1})\alpha(h)^{-1} \\ &= \sum_{k \in G} \alpha(k)\pi\alpha(k)^{-1} \\ &= \pi^G,\end{aligned}$$

where $k = gh$ runs over of all G since g does.

□

Remark 3.7. Notice that this averaging trick is quite general: if V is any representation of G, then the same argument shows that, given any vector $v \in V$, the vector

$$v^G = \sum_{g \in G} g(v)$$

is fixed by G. (It may however be zero – indeed this must happen if V is a non-trivial irreducible representation, as otherwise the span of v^G would be a proper subrepresentation.)

Definition 3.8. We say that a field k is *ordinary* for a finite group G if the order of G is invertible in k. If $|G|$ is not invertible in k then we say that the field is *modular* for G. Thus Maschke's theorem says that if k is ordinary for G, then any subrepresentation of a representation has a G-invariant complement.

Corollary 3.9 (Complete Reducibility)**.** *Let G be a finite group, and k a field in which $|G|$ is invertible. Then any k-linear representation of G is completely reducible, that is, it is a direct sum of irreducible subrepresentations.*

Proof. This follows immediately from Maschke's theorem and Lemma 3.1. □

Remark 3.10. For those who know some geometry: notice that projection maps allowed us to identify the set of all subspaces complementary to W with an affine subspace of the vector space End(V). By choosing different subspaces W,this essentially gives you charts for the Grassmanian of $(n-k)$-dimensional subspaces of V, where $\dim(V) = n$ and $\dim(W) = k$. Indeed to obtain actual charts one need only pick an arbitrary projection to W as "zero" to give the affine space the structure of a vector space. (If you have an inner product on V, then the orthogonal projection to W is a natural choice for such a zero.) Compare this to the construction of a manifold structure on $\mathrm{Gr}_k(V)$ that you have seen elsewhere.

Example 3.11. Recall the situation of Example 1.3: we let $V = \mathbb{C}[X]$ be the vector space of complex-valued functions on the set $X = \{1, 2, \ldots, n\}$, and $G = S_n$ acts via the formula $g(f)(i) = f(g^{-1}(i))$, for all $f \in \mathbb{C}[X], g \in G$ and $i \in \{1, 2 \ldots, n\}$. More explicitly, V has a basis $\{e_i\}_{1 \leq i \leq n}$ where $e_i(j) = 1$ if $i = j$ and 0 otherwise, and then the action of G is given by $g(e_i) = e_{g(i)}$ for each $i \in X$.

Notice that the function v given by $v(i) = 1$ for all $i \in \{1, 2, \ldots, n\}$ (thus in terms of the basis above, $v = e_1 + e_2 + \ldots e_n$) is fixed by G, so that $L = \langle v \rangle$ the line spanned by e is an invariant subspace of $\mathbb{C}[X]$. If we let

$$W = \{f \in \mathbb{C}[X] : \sum_{1 \leq i \leq n} f(i) = 0\},$$

then it is easy to see that W is G-invariant, and moreover W is a complement to L in V, that is, $V = L \oplus W$. Indeed if $f = \lambda v$ then $\sum_{i=1}^n f(i) = n\lambda$, which is zero exactly when $\lambda = 0$. Clearly L is an irreducible representation, and we shall see later that W is also, so that we have decomposed V into a direct sum of irreducibles.

Notice that even though X is a transitive G-set, the linear representation $\mathbb{C}[X]$ attached to it is not irreducible. (Indeed it is easy to see that for a general finite group G and transitive G-set X, the linear representation $\mathbb{C}[X]$ will always contain the trivial representation as a summand.)

LINEAR REPRESENTATIONS: SCHURS' LEMMA AND CHARACTER THEORY

KEVIN MCGERTY

We have now established that any representation is a direct sum of irreducible representations, so that in order to classify representations, it is enough to classify the irreducible ones. (This is much the same as the way we were able to reduce the classification of G-sets to the classification of transitive G-sets.) In this section we study irreducible representations, by considering the space of G-equivariant maps between them. As a consequence, for example, we will be able to give a criterion to check if a given representation is irreducible. (Recall in the previous section we decomposed the natural permutation representation of S_n into two pieces, one of which was irreducible, but we did not established the same property for the other summand.)

Another question we will address is uniqueness: we have shown that any representation V of a finite group G over $\mathbb{C}$ is a direct sum of irreducible subrepresentations. To what extent is the decomposition of V into irreducible summands unique? Already just by considering the direct sum of two copies of the trivial representation of G, we see that there cannot be uniqueness in general, but we will obtain a somewhat weaker statement: a slightly coarser decomposition of V into *isotypical* subrepresentations *is* unique. This will also imply that the the decomposition of V into irreducibles is unique up to isomorphism.

1. Schur's Lemma

In this section k *is an arbitrary field unless otherwise stated.*

We begin with a following lemma which, while very easy to prove, is of fundamental importance.

Lemma 1.1 (Schur). *Let V and W be representations of G, and suppose that $\phi\colon V \to W$ is a G-equivariant map. Then if V is irreducible, ϕ is either zero or injective, while if W is irreducible, then ϕ is either zero or surjective. In particular, if V and W are both irreducible then ϕ is either zero or an isomorphism.*

Proof. The subspace $\ker(\phi)$ is a G-subrepresentation of V: indeed if $\phi(v) = 0$, then $\phi(g(v)) = g(\phi(v)) = 0$, so that $g(v) \in \ker(\phi)$. Similarly $\mathrm{im}(\phi)$ is a G-subrepresentation of W. If V is irreducible the $\ker(\phi)$ must either be $\{0\}$ or all of V, hence ϕ is injective or zero. In the same way, if W is irreducible then $\mathrm{im}(\phi)$ is either $\{0\}$ or all of W, so that ϕ is zero or surjective. $\square$

An easy consequence of this (which is sometimes also called Schur's Lemma) is the following result. Recall that for G-representations V, W. we write $\mathrm{Hom}_G(V, W)$ is the space of G-equivariant linear maps from V to W. If $V = W$ we may also write $\mathrm{End}_G(V)$.

Date: January 2009.

Corollary 1.2. *Suppose that* k *is an algebraically closed field. Then if* V *is an irreducible* G*-representation* $\mathrm{End}_G(V) = \mathsf{k}$*. Moreover if* V *and* W *are irreducible representations then* $\mathrm{Hom}_G(V,W)$ *is either zero or one-dimensional.*

Proof. Suppose that $\phi \in \mathrm{End}_G(V)$. Then since k is algebraically closed, ϕ has an eigenvector λ say. But then $\phi - \lambda \in \mathrm{End}_G(V)$, and has a non-trivial kernel, so in particular it is not an isomorphism. But then by Schur's lemma, it must be zero, that is $\phi = \lambda$ as claimed.

To see the last part, note that if V and W are not isomorphic, Schur's lemma shows that $\mathrm{Hom}_G(V,W) = 0$. On the other hand, if $V \cong W$, then picking $\phi \in \mathrm{Hom}_G(V,W)$, we see that $\alpha \mapsto \phi^{-1} \circ \alpha$ gives and isomorphism between $\mathrm{Hom}_G(V,W)$ and $\mathrm{End}_G(V)$, which hence $\mathrm{Hom}_G(V,W)$ is one-dimensional as required. $\square$

Note that if k is not algebraically closed, then all we can conclude from Schur's lemma is that $\mathrm{End}_G(V)$ is a division algebra (or skew-field), that is, the nonzero elements of $\mathrm{End}_G(V)$ are all invertible (so that $\mathrm{End}_G(V)$ is like a field, except that the multiplication is not necessarily commutative).

Example 1.3. Suppose that $G = \mathbb{Z}/3\mathbb{Z}$ is the cyclic group of order 3. Then $\rho(1) = R$ where

$$R = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

(the matrix of rotation by $2\pi/3$ about 0) defines a representation of G on $\mathbb{R}^2$ which is irreducible (over $\mathbb{R}$). It is easy to see that $\mathrm{End}_G(\mathbb{R}^2) \cong \mathbb{C}$ in this case. Since we are primarily interested in the case $\mathsf{k} = \mathbb{C}$, we will mostly just assume that k is algebraically closed.

To show how useful Schur's lemma is, we now use it to describe the representations of Abelian groups in ordinary characteristic (over an algebraically closed field). We already know that any representation is completely reducible, so that it is enough to understand the irreducible representations.

Lemma 1.4. *Suppose that* k *is algebraically closed, and* G *is an Abelian group. If* (V,α) *is an irreducible representation of* G *then* V *is one-dimensional.*

Proof. Let $g \in G$. Since G is Abelian, $\alpha(g)$ commutes with $\alpha(h)$ for all $h \in G$, and so $\alpha(g) \in \mathrm{End}_G(V)$. But then by the corollary to Schur's lemma, $\alpha(g)$ is a scalar. Since g was arbitrary, we see that $\alpha(g) \in \mathsf{k}$ for all $g \in G$, and hence since V is irreducible, V must have dimension 1 as required. $\square$

Note that our previous example shows that this result is false if we do not assume k is algebraically closed. If G is a cyclic group $\mathbb{Z}/n\mathbb{Z}$, then the one-dimensional representations of G are given by picking a $\zeta \in \mathsf{k}$ such that $\zeta^n = 1$. Hence if k contains ζ a primitive n-th root of unity (for example $e^{2\pi i/n}$ when $\mathsf{k} = \mathbb{C}$), the irreducible representations of $\mathbb{Z}/n\mathbb{Z}$ are given by the set $\{\zeta^k : 1 \leq k \leq n\}$. Since any Abelian group can be written as a product of cyclic groups, say $G = \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ we see that the irreducible G-representations are given by r-tuples $(\zeta_1^{i_1}, \dots, \zeta_r^{i_r})$ where ζ_i is a primitive n_i-th root of unity, and $1 \leq i_j \leq n_j$. Thus we see there are exactly $|G|$ irreducible representations of an Abelian group G[1]. We summarize this in the following proposition.

Proposition 1.5. *Let G be a finite abelian group, and suppose that k is an algebraically closed field which is ordinary for G. Then all the irreducible representations of G are 1-dimensional, and there are $|G|$ distinct irreducible representations.*

The example of S_3 which we already worked out using just linear algebra shows that for non-Abelian groups the number of irreducible representations can be smaller than $|G|$ (indeed $|S_3| = 6$, whereas we found 3 irreducible representations). You might wish to take a guess at what the number of irreducible representations actually is...

As another application of the the rigidity of irreducible representations, we prove the converse to a result of the previous section: if V is a sum of irreducible representations then any subrepresentation has an G-invariant complement. (Of course this is Maschke's theorem in the case where the order of the group is invertible in the field we are working over, but the proof below does not assume that G is finite, or indeed anything about the field k, only that the representations in question are finite dimensional). The proof is not an application of Schur's lemma, but it uses the same circle of ideas.

Lemma 1.6. *Suppose that V is a sum of irreducible representations of G. Then any subrepresentation of V has a G-invariant complement.*

Proof. Suppose that W is a proper subrepresentation of V, and consider the set $\mathcal{S}$ of all subrepresentations U of V such that $W \cap U = \{0\}$, so that the sum $W + U$ is direct. Pick U of maximal dimension in $\mathcal{S}$ (possibly we have $\dim(U) = 0$). Then either $W \oplus U = V$, in which case we are done, or $W \oplus U = W'$ is a proper subspace of V. But in that case, it cannot be that every irreducible subrepresentation of V lies in W', since V is the direct sum of irreducible subrepresentations. Thus there must be some irreducible subrepresentation N with N not contained in W'. But then $N \cap W'$ is a proper subrepresentation of N, and hence by the irreducibility of N, it must be zero. Then the sum $W' + N$ is direct. But then

$$(W \oplus U) \oplus N = W \oplus (U \oplus N)$$

is a direct sum and $(U \oplus N)$ has strictly greater dimension than U, which contradicts the choice of U. $\square$

Remark 1.7. Note that we only assumed that V was a sum of irreducible representations, not a direct sum. Thus it actually follows from this Lemma and the proof that Maschke's theorem implies complete reducibility that if V is a sum of irreducible subrepresentations, then it must in fact be a direct sum of irreducible subrepresentations.

Next we use Schur's lemma to show that there are only finitely many isomorphism classes of irreducible representations of a finite group G. Recall that if X is a finite G-set, the space of functions on X is naturally a representation of G. Taking $X = G$ with the left action of G on itself, we see that $\mathbb{C}[G]$, the space of functions

[1]If k doesn't contain the appropriate primitive roots of unity, then this conclusion fails. If $\mathsf{char}(\mathsf{k}) = p$ and p divides n_i this always happens (as then $x^p - 1 = (x-1)^p$), so we see that it is not enough for k to be algebraically closed: the result only holds for ordinary fields for G.

on G is a representation of G. This is called the *regular representation*. It has a basis $\{e_h : h \in G\}$, and the action of G in terms of this basis is $g(e_h) = e_{gh}$, for $g, h \in G$.

Lemma 1.8. *Suppose that* k *is ordinary for* G*, and let* V *be an irreducible representation of* G*. Then* V *isomorphic to a subrepresentation of* $\mathsf{k}[G]$*.*

Proof. Pick a vector $v \in V$, and let $\phi \colon \mathsf{k}[G] \to V$ be given by $e_g \mapsto g(v)$. Then it is easy to see that this map is G-equivariant: indeed

$$\phi(g(e_h)) = \phi(e_{gh}) = (gh).v = g(h.v) = g(\phi(e_h)).$$

But since $\phi(e_e) = v$ we see that $\phi \neq 0$, so that as V is irreducible, Schur's lemma implies that ϕ is surjective. Now $\ker(\phi)$ is a subrepresentation of $\mathsf{k}[G]$, and so by Maschke's theorem it has a G-invariant complement U in $\mathsf{k}[G]$. But then ϕ induces an isomorphism from U to V, and we are done. $\square$

Remark 1.9. Notice that this gives a concrete bound of at most $|G|$ irreducible representations, which is exactly what we saw for Abelian groups. Moreover we now see that to understand all the irreducible representations of G it is enough to decompose the regular representation into irreducibles.

Remark 1.10. If k is an arbitrary field, not necessarily ordinary for G (or indeed even algebraically closed), then the previous theorem still shows that any irreducible representation is a quotient of $\mathsf{k}[G]$.

2. Homomorphisms and the isotypical decomposition

In this section we assume that k *is algebraically closed and ordinary for* G.

We can now also establish a decomposition of any representation into summands which are canonical. Take a set of irreducible representations $\{U_j : j \in J\}$ such that any irreducible is isomorphic to exactly one U_j (so that by what we have just shown, J is a finite set).

Now suppose that V is a representation of G. Then we may decompose $V = \bigoplus_{i=1}^n V_i$ into a direct sum of irreducible representations (not necessarily in a unique way). For each $j \in J$ let $V^j = \bigoplus V_i$ where the sum is over the V_i such that $V_i \cong U_j$. The decomposition $V = \bigoplus_{j \in J} V^j$ is known as an *isotypical decomposition* of V. It is unique, whereas the decomposition $V = \bigoplus_i V_i$ into irreducible subrepresentations is not.

Lemma 2.1. *Let* V *and* W *be representations of* G*, and suppose that* $\bigoplus_j V^j$ *and* $\bigoplus_j W^j$ *are isotypical decompositions of* V *and* W *respectively. Then if* $\phi \in Hom_G(V, W)$ *we have* $\phi(V_j) \subseteq W_j$*. In particular, the isotypical decomposition is unique.*

Proof. For $k \in J$ let $\iota_k \colon V^k \to V$ be the inclusion of V^k into V, and similarly let $\pi_l \colon W \to W^l$ be the projection from W to the l-th summand W^l. Given $\phi \in \mathrm{Hom}_G(V, W)$ let $\phi_{kl} \colon V^k \to W^l$ be the map $\pi_l \circ \phi \circ \iota_k$. Thus $(\phi_{kl})_{k,l \in J}$ is the "block matrix" decomposition of ϕ according to the isotypic summands V_k and W_l.

Decomposing (arbitrarily) each V_k and W_l into irreducible subrepresentations, and then using Schur's lemma we immediately see that $\phi_{kl} = 0$ when $k \neq l$, and so $\phi(V^j) \subset W^j$ as required. To see that this implies the isotypical decomposition is unique, apply the first part of the lemma to the identity map $\mathrm{id} \colon V \to V$. $\square$

Remark 2.2. Note that while the decomposition of V into irreducible subrepresentations is not unique, the decomposition of V into irreducibles is unique *up to isomorphism*, since the decomposition $V = \bigoplus_{j \in J} V^j$ is unique, and we have $V^j \cong U_j^{\oplus d_j}$ where d_j can be calculated from the dimension of V^j, indeed $d_j = \dim(V^j)/\dim(U_j)$.

Example 2.3. Recall our description of the representations of

$$S_3 = \langle s, t : s^2 = t^3 = 1, sts^{-1} = t^{-1} \rangle.$$

over a field k of characteristic greater than 3. A representation of S_3 on a vector space V is given by a pair of linear maps S, T satisfying the relations $S^2 = T^3 = \mathrm{Id}_V$ and $STS^{-1} = T^{-1}$, and we can decompose V according to the eigenvalues of the matrices S and T (the linear maps S and T are diagonalizable since $\mathrm{char}(\mathsf{k}) \neq 2, 3$). Indeed taking ω a primitive 3rd root of unity, we set

$$\begin{aligned} W_1 &= \{v \in V : S(v) = T(v) = v\}, \quad W_{-1} = \{v \in V : S(v) = v, T(v) = -v\}, \\ V_{\omega^{\pm 1}} &= \{v \in V : T(v) = \omega^{\pm 1} v\}. \end{aligned}$$

Each of these subspaces is a subrepresentation, and they give the isotypical decomposition of V: the subrepresentation W_1 is the direct sum of copies of the trivial representation, the subrepresentation W_{-1} is a direct sum of the one-dimensional representation where s acts as -1 and t acts as 1, while $V_{\omega^{\pm 1}}$ is a direct sum of copies of the irreducible two-dimensional representation.

Note that while the decomposition of V into these three subspaces involves no choices, to decompose V further into irreducible subrepresentations we must choose an arbitrary decomposition of W_1 and W_{-1} into one-dimensional subspaces and $V_{\omega^{\pm 1}}$ into 2-dimensional subrepresentations (which can be done as we did previously by choosing a basis of the ω-eigenspace of T). On the other hand, given any two such choices of a decomposition, we can find a G-equivariant isomorphism of V to itself which interchanges them, which verifies that the decomposition of V into irreducibles is unique up to isomorphism.

Schur's lemma in fact gives us a complete description of what the space of equivariant homomorphisms between two G-representations looks like. Indeed by the previous lemma on the isotypic decomposition, we need only consider representations which are isotypic, and the next lemma deals with this case.

Lemma 2.4. *Let $V \cong U^{\oplus n}$ and $W \cong U^{\oplus m}$ be G-representations, where U is irreducible. Then*

$$\mathit{Hom}_G(V, W) \cong \mathit{Mat}_{n,m}(\mathsf{k}).$$

Proof. We use a block matrix decomposition again. Let $V = \bigoplus_{i=1}^n V_i$ where $V_i \cong U$ for all i, and similarly $W = \bigoplus_{j=1}^m W_j$ with $W_j \cong U$ for all j. Then for i, j with $1 \leq i \leq n$ let $\iota_i \colon V_i \to V$ be the inclusion of V_i into V as the i-th term of the direct sum, and let $\pi_j \colon W \to W_j$ be the projection from W to the j-th summand W_j. Given $\phi \in \mathrm{Hom}_G(V, W)$ let $\phi_{ij} \colon V_i \to W_j$ be the map $\pi_j \circ \phi \circ \iota_i$. If we fix an isomorphism $V_i \cong U$ and $W_j \cong U$ for each i, j, then we obtain isomorphisms $\mathrm{Hom}_G(V_i, W_j) \cong \mathrm{Hom}_G(U, U = \mathsf{k}$, where the last equality follows from Schur's lemma. Hence we may identify each ϕ_{ij} with a scalar, λ_{ij} say. Then the map $\phi \mapsto (\lambda_{ij})$ gives the required isomorphism. $\square$

Remark 2.5. Note that the isomorphism given in the previous lemma is not unique, in the same way that if V and W are vector spaces of dimension n and m respectively, then $\mathrm{Hom}(V,W)$ is isomorphic to $\mathrm{Mat}_{n,m}(\mathsf{k})$, but one must pick bases of V and W in order to define an isomorphism.

Let us put the two previous lemmas together to give an explicit description of $\mathrm{Hom}_G(V,W)$ for two arbitrary representations of G.

Proposition 2.6. *Let V and W be linear representations of G, and let $V = \bigoplus_{j\in J} V^j$, and $W = \bigoplus_{j\in J} W^j$ be their isotypical decompositions. Then if $V^j \cong U_j^{\oplus n_j}$ and $W^j \cong U_j^{\oplus m_j}$ for integers $n_j, m_j, (j \in J)$ we have*

$$\mathit{Hom}_G(V,W) \cong \bigoplus_{j\in J} \mathit{Mat}_{n_j,m_j}(\mathsf{k}).$$

Proof. By Lemma 2.1 we see immediately that

$$\mathrm{Hom}_G(V,W) = \bigoplus_{j\in J} \mathrm{Hom}_G(V^j, W^j),$$

and then using Lemma 2.4 we see that the j-th term in this sum is isomorphic to $\mathrm{Mat}_{n_j,m_j}(\mathsf{k})$ as required. □

Now let's extract some numerical information from this. Let $V \cong \bigoplus_{j\in J} U_j^{\oplus n_j}$. Taking $V = W$ in the Proposition 2.6 it ifollows immediately that

$$\dim(\mathrm{Hom}_G(V,V)) = \sum_{j\in J} n_j^2. \tag{2.1}$$

We can use this to give a numerical criterion for a representation to be irreducible.

Corollary 2.7. *Suppose that V is a representation of G. Then V is irreducible if and only if*

$$\dim(\mathit{Hom}_G(V,V)) = 1.$$

Proof. We use the notation of the previous paragraph. Equation 2.1 shows that the dimension of $\mathrm{Hom}_G(V,V)$ is $\sum_{j\in J} n_j^2$. Such a sum of squares is equal to 1 if and only if exactly one of the n_js is 1 and all the rest are zero, that is, when V is irreducible. □

Recall that if V and W are G-representations, then $\mathrm{Hom}(V,W)$, the space of all linear maps from V to W, is a G-representation, and moreover, the space of G-equivariant linear maps $\mathrm{Hom}_G(V,W)$ is just the subspace of $\mathrm{Hom}(V,W)$ on which G acts trivially. Thus rephrasing our condition above, we see that to show that a representation V is irreducible, we need only show that the trivial representation occurs exactly once in $\mathrm{Hom}(V,V)$.

Definition 2.8. Let (V,ρ) be a G-representation. Then the subspace

$$V^G = \{v \in V : \rho(g)(v) = v, \forall g \in G\},$$

is the isotypic summand corresponding to the trivial representation. It is known as the space of G-invariants in V. If V, W are G-representations, then $\mathrm{Hom}_G(V,W)$ is by definition $\mathrm{Hom}(V,W)^G$.

Although we now have a numerical criterion for irreducibility, it is not yet clear that it is a particularly useful or computable one. In fact an idea we have already used in the proof of Maschke's lemma will allows us to turn this criterion into a very computable one. Recall that the key to that proof was to average an arbitrary projection to obtain a G-equivariant one. We now formalize this averaging trick using $\mathbb{C}[G]$, the space of complex-valued functions on G. Thus we take a short detour to study the properties of $\mathbb{C}[G]$.

3. The group algebra

In this section we assume that k *is ordinary for* G*, that is* k *is algebraically closed and* $|G|$ *is invertible in* k.

The vector space $\mathsf{k}[G]$ of functions on G has more structure that just a linear action of G.

Definition 3.1. A k-algebra is a (not necessarily commutative) ring A which contains k as a central commutative subring, so that $\lambda.x = x.\lambda$ for all $x \in A, \lambda \in \mathsf{k}$. Thus in particular A is a k-vector space. Given two k-algebras A and B, a homomorphism of k-algebras is a k-linear map $\alpha\colon A \to B$ which respects multiplication and maps the identity element in A to that in B, that is,

$$\alpha(x.y) = \alpha(x).\alpha(y), \quad \forall x, y \in A; \quad \alpha(1_A) = 1_B.$$

Example 3.2. Let V be a k-vector space. Then the space $\mathrm{End}_{\mathsf{k}}(V)$ of linear maps from V to itself is a k-algebra.

We can make $\mathbb{C}[G]$ into a k-algebra using a *convolution product*[2]: namely we may define $\star\colon \mathbb{C}[G] \times \mathbb{C}[G] \to \mathbb{C}[G]$ by

$$(f \star g)(k) = \sum_{h \in G} f(kh^{-1}).g(h),$$

for any $k \in G$. More concretely, using the basis $\{e_g : g \in G\}$ of indicator functions, you can check that

$$e_g \star e_h = e_{gh}, \quad \forall g, h \in G \tag{3.1}$$

Thus e_e the indicator function of the identity element of G is the unit in $\mathsf{k}[G]$, so that the field k is embedded in $\mathsf{k}[G]$ by the map $\lambda \mapsto \lambda e_e$.

Given a representation (V, ρ) of G, we can extend ρ to a map, which we also write as ρ, from $\mathsf{k}[G] \to \mathrm{End}(V)$ given by

$$f \mapsto \sum_{g \in G} f(g)\rho(g).$$

It follows from Equation 3.1 that $\rho\colon \mathsf{k}[G] \to \mathrm{End}(V)$ is a map of k-algebras, that is

$$\rho(f \star g) = \rho(f) \circ \rho(g),$$

where on the right-hand side $\circ$ denotes composition of endomorphisms. In fact we can reformulate the study of G-representations in terms of the group algebra.

Lemma 3.3. *Let V be a* k*-vector space. Then giving a linear action of G on V is equivalent to giving an algebra map* $\mathsf{k}[G] \to$ *End*(V).

[2]You should compare this to the convolution product of functions you may have seen in Fourier theory: for f, g functions on $\mathbb{R}$, the convolution of f with g is $(f \star g)(x) = \int f(x-y)g(y)dy$.

Proof. We have already seen that given $\rho\colon G \to \mathrm{GL}(V)$, we may construct an algebra map from $\mathsf{k}[G] \to \mathrm{End}(V)$. Thus we need only check the converse. Suppose that $\rho\colon \mathsf{k}[G] \to \mathrm{End}(V)$. For $g \in G$ set $\rho_G(g) = \rho(e_g)$. Then since $\rho(e_g \star e_h) = \rho(e_g) \circ \rho(e_h)$ we see that

$$\rho_G(g.h) = \rho(e_{gh}) = \rho(e_g) \circ \rho(e_h) = \rho_G(g) \circ \rho_G(h).$$

But now since $\rho(e_e) = \mathrm{id}_V$, it follows that $\rho_G(g)$ is invertible for every $g \in G$ with inverse $\rho_G(g^{-1})$, and hence ρ_G is a homomorphism from G to $\mathrm{GL}(V)$ as required. □

We now use the group algebra to reformulate the averaging trick we used in the proof of Maschke's theorem. Let $I_G = |G|^{-1}\sum_{g\in G} e_g$, that is I_G is the function in $\mathbb{C}[G]$ which is equal to $|G|^{-1}$ on every point of G (thus we are assuming that $|G| \neq 0$ in k).

Lemma 3.4. *For any $g \in G$ we have $e_g \star I_G = I_G$, and hence $I_G^2 = I_G$. Moreover, if V is a G-representation, then $\rho(I_G)$ is the G-equivariant projection to the subspace V^G of V on which G acts trivially.*

Proof. We have

$$e_g \star I_G = e_g \star (|G|^{-1}\sum_{h\in G} e_h) = |G|^{-1}\sum_{h\in G} e_{gh} = |G|^{-1}\sum_{k\in G} e_k = I_G.$$

where $k = gh$ runs over all of G as h does. It is then clear that

$$I_G^2 = |G|^{-1}(\sum_{g\in G} e_g \star I_G) = |G|^{-1}\sum_{g\in G} I_G = I_G.$$

Now if (V,ρ) is a G-representation, it follows immediately that $\rho(I_G)$ is a projection operator (as $\rho(I_G)^2 = \rho(I_G^2) = \rho(I_G)$). Moreover, since $\rho(g) \circ \rho(I_G) = \rho(I_G)$ it is clear that G acts trivially on the image of $\rho(I_G)$, and also by the definition of I_G, if $\rho(g)(v) = v$ for all $g \in G$, then $\rho(I_G)(v) = v$. Thus $\rho(I_G)$ is the required projection. □

Remark 3.5. In the language we have just built up, our proof of Maschke's theorem took an arbitrary projection from V to the subrepresentation W and applied I_G to it (as an element of the representation $\mathrm{Hom}(V,V)$) to get an equivariant projection.

We are now finally able to make our irreducibility criterion more explicit: given a representation V, we wish to calculate $\dim(\mathrm{Hom}_G(V,V))$. By what we have shown above is that this dimension is just the rank of the projection operator I_G on the representation $\mathrm{Hom}(V,V)$. But the rank of a projection map is simply its trace, so that we find

$$\dim(\mathrm{Hom}_G(V,V)) = \mathrm{tr}(I_G, \mathrm{Hom}(V,V)).$$

Moreover, since trace is linear, it follows that

$$\dim(\mathrm{Hom}_G(V,V)) = |G|^{-1}\sum_{g\in G} \mathrm{tr}(g, \mathrm{Hom}(V,V)).$$

We summarize the above into the following proposition.

Proposition 3.6. *Let (V, ρ) be a G-representation. Then*

$$\dim(Hom_G(V,V)) = |G|^{-1} \sum_{g \in G} tr(g, Hom(V,V)),$$

thus in particular V is irreducible if and only if

$$|G|^{-1} \sum_{g \in G} tr(g, Hom(V,V)) = 1$$

Example 3.7. Consider the symmetric group S_n and the set $X = \{1, 2, \dots, n\}$ on which it acts. We already decomposed the permutation representation $\mathbb{C}[X]$ into two pieces:

$$\mathbb{C}[X] = \mathbb{C}\langle v \rangle \oplus \{f \in \mathbb{C}[X] : \sum_{1 \leq i \leq n} f(i) = 0\}.$$

where $v = \sum_{i=1}^{n} e_i$. We are now able to show that this decomposition is in fact into irreducible subrepresentations.

Indeed these are distinct irreducible representations if and only if

$$\dim(\mathrm{Hom}_G(\mathbb{C}[X], \mathbb{C}[X])) = 2.$$

To calculate $\dim(\mathrm{Hom}_G(\mathbb{C}[X], \mathbb{C}[X]))$ we need only calculate the sum of the traces $\mathrm{tr}(g, \mathrm{Hom}(\mathbb{C}[X], \mathbb{C}[X]))$ for each $g \in S_n$. Let $\{e_i : 1 \leq i \leq n\}$ be the basis of indicator functions for $\mathbb{C}[X]$. Then we can define a natural basis $\{e_{ij} : 1 \leq i, j \leq n\}$ of $\mathrm{Hom}(\mathbb{C}[X], \mathbb{C}[X])$ in terms of this basis, such that $e_{ij}(e_k) = e_j$ if $k = i$ and zero otherwise. It is easy to check that $g(e_{ij}) = e_{g(i),g(j))}$.

It follows from this that if we calculate the trace of $g \in S_n$ on the basis $\{e_{ij} : 1 \leq i, j \leq n\}$ then

$$\mathrm{tr}(g, \mathrm{Hom}(V,V)) = |\{(i,j) : 1 \leq i, j \leq n, g(i) = i, g(j) = j\}|,$$

since the diagonal entry $((ij), (ij))$ will be zero or 1 according to whether $g(i) = i$ and $g(j) = j$ or not. Hence

$$\dim(\mathrm{Hom}_G(V,V)) = |G|^{-1} \sum_{g \in G} F_{X \times X}(g),$$

where $F_{X \times X}(g)$ is the number of fixed points of S_n on the set $X \times X$. But now Burnsides theorem says that this is just the number of orbits of S_n on $X \times X$. But this is clearly 2: the pairs $\{(i,i) : 1 \leq i \leq n\}$ form one orbit, while the pairs $\{(i,j) : i \neq j\}$ form the other.

4. Character Theory

In this section k *is assumed to be ordinary for G.*

Given a linear map $\alpha \colon V \to V$, there are a number of natural invariants associated to it: we may take its trace, its determinant, or perhaps most comprehensively its characteristic polynomial $\det(\lambda - \alpha)$. Thus given a group G acting linearly on V, we can attach to it these invariants for each group element. Since $\det \colon \mathrm{GL}(V) \to \mathsf{k}^{\times} = \mathrm{GL}_1(\mathsf{k})$ is a group homomorphism, the determinant map actually yields a new one-dimensional representation of G. However, since for example any perfect group[3] has no nontrivial one-dimensional representations we

[3] *i.e.* a group for which G which is equal to its own derived group $[G, G]$, which is the case for every non-Abelian simple group.

cannot expect that this will record much information about our original representation V. On the other hand, we have already seen in the last section that knowing traces of the elements of G (admittedly on $\mathrm{Hom}(V, V)$ not V) allows us to test if V is irreducible. In fact with not much more work we will be able to see that the traces yield a complete invariant of V.

Definition 4.1. Let (V, ρ) be a representation of G. Then the character of V is the k-valued function

$$\chi_V : G \to \mathsf{k}, \quad \chi_V(g) = \mathrm{tr}(\rho(g)).$$

Lemma 4.2. *Suppose that (V, ρ) is a representation of G. Then*

(1) *If $g \in G$ then $\rho(g)$ is diagonalizable. If $\mathsf{k} = \mathbb{C}$ then $\chi_V(g^{-1}) = \overline{\chi_V(g)}$, where the bar denotes complex conjugation.*
(2) $\chi_V(e) = \dim(V)$.
(3) *χ_V is conjugation-invariant, that is $\chi_V(ghg^{-1}) = \chi_V(h)$ for all $g, h \in G$.*
(4) *If V^* is the dual representation, then $\chi_{V^*}(g) = \chi_V(g^{-1})$.*
(5) *If V and W are G-representations then $\chi_{V \oplus W} = \chi_V + \chi_W$.*

Proof. Let $C = \langle g \rangle$ be the subgroup of G generated by g. It is clear that C, the group generated by g, is a finite cyclic subgroup of G, hence we see that as a C-representation, V splits as a direct sum of lines. Since $g \in C$ we immediately see that g is diagonalizable as required. Picking a basis $\{e_1, e_2, \ldots, e_n\}$ of eigenvectors of g, so that $g(e_i) = \lambda_i e_i$ say, we have $\chi_V(g) = \sum_{i=1}^n \lambda_i$. Since $\rho(g^{-1}) = \rho(g)^{-1}$ is diagonal on the same basis, with eigenvalues λ_i^{-1}, it follows $\chi_V(g^{-1}) = \sum_{i=1}^n \lambda_i^{-1}$. If $\mathsf{k} = \mathbb{C}$, then since $\rho(g)^{|G|} = \mathrm{id}$ for any $g \in G$, the eigenvalues of $\rho(g)$ are roots of unity, and hence they have modulus 1. But if $z \in \mathbb{C}$ has $|z| = 1$ then $z^{-1} = \bar{z}$, and since complex conjugation is linear, it follows that $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

The second part is clear, since $\rho(e) = \mathrm{id}_V$ and the trace of the identity endomorphism is clearly just the dimension of V. For the third part, if $g, h \in G$ then

$$\chi_V(ghg^{-1}) = \mathrm{tr}(\rho(ghg^{-1})) = \mathrm{tr}(\rho(g)\rho(h)\rho(g)^{-1}) = \mathrm{tr}(\rho(h)) = \chi_V(h).$$

since $\mathrm{tr}(\alpha\beta) = \mathrm{tr}(\beta\alpha)$ for all $\alpha, \beta \in \mathrm{End}(V)$.

For the fourth part suppose $\alpha \colon V \to V$ is a linear map. If A is the matrix of α with respect to some basis of V, then the matrix of α^t with respect to the corresponding dual basis of V^* is A^t. But clearly $\mathrm{tr}(A) = \mathrm{tr}(A^t)$, so $\mathrm{tr}(\alpha) = \mathrm{tr}(\alpha^t)$. Now if $g \in G$, then $\rho^*(g) = \rho(g^{-1})^t$, hence we see

$$\chi_{V^*}(g) = \mathrm{tr}(\rho(g^{-1})^t) = \mathrm{tr}(\rho(g^{-1})) = \chi_V(g^{-1}),$$

as claimed.

Finally, if $U = V \oplus W$ and $\alpha \colon U \to U$ preserves each of V and W, then picking a basis of V and a basis of W their union is a basis of U with see that with respect to this basis the matrix of α has the form

$$\left(\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}\right)$$

Thus clearly $\mathrm{tr}(\alpha) = \mathrm{tr}(\alpha_{|V}) + \mathrm{tr}(\alpha_{|W})$. Applying this observation to each $\rho(g)$ part four is now clear. $\square$

Definition 4.3. A function $f \in \mathsf{k}[G]$ is said to be a *class function* if $f(ghg^{-1}) = f(h)$, that is, if f is constant on the conjugacy classes of G. Let $\mathcal{C}_\mathsf{k}(G)$ denote the space of class functions on G. The space $\mathcal{C}_\mathsf{k}(G)$ has an obvious basis: for a conjugacy class

$\mathcal{C} \subseteq G$ let $z_{\mathcal{C}}$ be the indicator function of $\mathcal{C}$, so that $z_{\mathcal{C}} = \sum_{g \in \mathcal{C}} e_g$. Clearly the set $\{z_{\mathcal{C}} : \mathcal{C} \text{ a conjugacy class of } G\}$ is a basis of $\mathcal{C}_{\mathsf{k}}(G)$. Thus

$$\dim(\mathcal{C}_{\mathsf{k}}(G)) = |\{\mathcal{C} : \mathcal{C} \subseteq G \text{ a conjugacy class}\}|$$

The previous lemma shows that if V is a representation, then χ_V is a class function on G, thus at first sight it might seem to hold rather little information. However our study of G-equivariant maps between representations in terms of the element $I_G \in \mathsf{k}[G]$ suggests otherwise. Indeed if V and W are representations, then we have

$$\begin{aligned}\dim(\mathrm{Hom}_G(V, W)) &= \dim(\mathrm{Hom}(V, W)^G) \\ &= \mathrm{tr}(I_G, \mathrm{Hom}(V, W)) \\ &= |G|^{-1} \sum_{g \in G} \mathrm{tr}(g, \mathrm{Hom}(V, W)) \\ &= |G|^{-1} \sum_{g \in G} \chi_{\mathrm{Hom}(V,W)}(g).\end{aligned} \tag{4.1}$$

Thus if we can determine the character of $\mathrm{Hom}(V, W)$ in terms of that of V and W, we will be able to calculate the dimension of the space of equivariant maps between V and W.

Proposition 4.4. *Suppose that V and W are finite-dimensional G-representations. Then*

$$tr(g, Hom(V, W)) = \chi_V(g^{-1})\chi_W(g), \quad \forall g \in G.$$

Proof. Let $g \in G$. The action of g on V and W is diagonalizable, thus we may pick bases $\{e_1, e_2, \dots, e_n\}$ and $\{f_1, f_2, \dots, f_m\}$ of V and W respectively such that $g(e_i) = \lambda_i e_i$ and $g(w_j) = \mu_j w_j$ for some scalars $\lambda_i, \mu_j \in \mathsf{k}$. Calculating the trace of g^{-1} on V and g on W with respect to these bases we see

$$\chi_V(g^{-1}) = \sum_{1 \leq i \leq n} \lambda_i^{-1}, \quad \chi_W(g) = \sum_{1 \leq j \leq m} \mu_j.$$

Now $\mathrm{Hom}(V, W)$ has a basis $\{e_i^* f_j : 1 \leq i \leq n, 1 \leq j \leq m\}$, where $e_i^* f_j(v) = e_i^*(v) f_j$ for any $v \in V$. But $g(e_i^* f_j)(v) = e_i^*(g^{-1}(v))g(f_j) = \lambda_i^{-1}\mu_j e_i^* f_j(v)$ for all $v \in V$, so that the functions $e_i^* f_j$ are eigenvectors for the action of g. Thus calculating the trace of g using this basis we see

$$\begin{aligned}\mathrm{tr}(g, \mathrm{Hom}(V, W)) &= \sum_{i,j} \lambda_i^{-1}\mu_j \\ &= (\sum_{1 \leq i \leq n} \lambda_i^{-1}).(\sum_{1 \leq j \leq m} \mu_j) \\ &= \chi_V(g^{-1})\chi_W(g).\end{aligned}$$

□

Motivated by this, we define a symmetric bilinear form on $\mathsf{k}[G]$. For $f \in \mathsf{k}[G]$ set $f^*(k) = f(k^{-1})$, and define

$$\begin{aligned}\langle f, g \rangle = |G|^{-1} \sum_{k \in G} f^*(k)g(k) &= |G|^{-1} \sum_{k \in G} f(k)g^*(k) \\ = |G|^{-1} \sum_{\substack{k_1, k_2 \in G \\ k_1.k_2 = 1}} f(k_1)g(k_2) &= |G|^{-1}(f \star g)(e).\end{aligned}$$

Note the map $f \mapsto f^*$ preserves the form $\langle -, - \rangle$ since $(f^*)^* = f$. The form $\langle -, - \rangle$ it is obviously nondegenerate since

$$\langle e_g, e_h \rangle = \begin{cases} |G|^{-1} & \text{if } g = h^{-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Equivalently $\{e_g : g \in G\}$ and $\{|G|e_g^* : g \in G\}$ are dual bases.

In fact it is the restriction of $\langle -, - \rangle$ to $\mathcal{C}_{\mathsf{k}}(G)$ which is most important for us. To better understand the form on $\mathcal{C}_{\mathsf{k}}(G)$, note that since conjugation is a group homomorphism, the inverse map induces a map on the set of conjugacy classes, and hence the map $f \mapsto f^*$ restricts to an endomorphism of $\mathcal{C}_{\mathsf{k}}(G)$. It is easy to see that

$$\langle z_{\mathcal{C}}, z_{\mathcal{D}} \rangle = \begin{cases} |\mathcal{C}|/|G|, & \text{if } z_{\mathcal{D}} = z_{\mathcal{C}}^*, \\ 0, & \text{otherwise.} \end{cases}$$

Thus $\langle -, - \rangle$ restricts to a nondegenerate symmetric form on $\mathcal{C}_{\mathsf{k}}(G)$ with $\{z_{\mathcal{C}}\}$ and $\{|\mathcal{C}|/|G|z_{\mathcal{C}}^*\}$ as dual bases.

Theorem 4.5. *Let V and W be representations of G with characters χ_V and χ_W respectively. Then*

$$\dim(\mathit{Hom}_G(V, W)) = \langle \chi_V, \chi_W \rangle.$$

In particular, if V and W are irreducible then

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

Proof. This is an immediate consequence of the previous lemma and Equation 4.1. □

This last theorem is remarkably powerful. We note now some of its important consequences.

Corollary 4.6. *Let $\{U_j : j \in J\}$ be a complete set of irreducible G-representations. Then the characters $\chi_j := \chi_{U_j} \in \mathcal{C}_{\mathsf{k}}(G)$ are linearly independent.*

Proof. Suppose that $\sum_{j \in J} a_j \chi_j = 0$ for some $a_j \in \mathsf{k}$. Then we have

$$0 = \langle \sum_{j \in J} a_j \chi_j, \chi_i \rangle = a_i,$$

for each $i \in J$. □

Notice that this gives a new bound on the number of irreducible representations: since the characters of nonisomorphic irreducible representations are linearly independent, their number is at most the dimension of $\mathcal{C}_{\mathsf{k}}(G)$, which is just the number of conjugacy classes in G. For non-Abelian groups G, this is an improvement on our earlier bound of $|G|$.

Corollary 4.7. *Let V be a G-representation. Then χ_V the character of V determines V up to isomorphism.*

Proof. If $\{U_j : j \in J\}$ is a complete set of irreducible G-representations, then by complete reducibility we know that $V \cong \bigoplus_{j \in J} U_j^{\oplus n_j}$. Thus V is determined up to isomorphism by the numbers $\{n_j : j \in J\}$. But we have already seen by our study of G-equivariant homomorphisms that

$$n_j = \dim(\mathrm{Hom}_G(V, U_j)),$$

and hence by Theorem 4.5 we have $n_j = \langle \chi_V, \chi_{U_j} \rangle$. □

We now use character theory to give a more explicit description of the isotypical decomposition of a representation. Recall that $\mathsf{k}[G]$ is an algebra (the group algebra). The space of class functions has a natural description in terms of the algebra structure on $\mathsf{k}[G]$. If A is a k-algebra, we set

$$Z(A) = \{z \in A : xz = zx, \forall x \in A\}.$$

The set $Z(A)$ is called the *centre* of A. It is easy to check that $Z(A)$ is a (commutative) subalgebra of A.

Lemma 4.8. *The centre of the group algebra $\mathsf{k}[G]$ is the space of class functions $\mathcal{C}_\mathsf{k}(G)$.*

Proof. Recall that $\mathsf{k}[G]$ has a basis $\{e_g : g \in G\}$ and the multiplication in $\mathsf{k}[G]$ is given by $e_g.e_h = e_{gh}$. If $z = \sum_{k \in G} \lambda_k e_k$, then z is in $Z(A)$ if and only if we have $e_g.z = z.e_g$ for all $g \in G$. But since e_g is invertible with inverse $e_{g^{-1}}$ this is equivalent to the condition $e_g z e_{g^{-1}} = z$ for every $g \in G$. Now since $e_g e_k e_{g^{-1}} = e_{gkg^{-1}}$ this is equivalent to

$$\sum_{k \in G} \lambda_k e_{gkg^{-1}} = \sum_{k \in G} \lambda_k e_k, \quad \forall g \in G.$$

Thus $z \in Z(A)$ if and only if $\lambda_k = \lambda_{gkg^{-1}}$ for all $g \in G$, that is, if and only if z is a class function. □

Lemma 4.9. *Let (V, ρ) be an irreducible representation of G, and let $f \in \mathcal{C}_\mathsf{k}(G)$. Then we have*

$$\rho(f) = \frac{|G|}{\dim(V)} \langle f, \chi_V^* \rangle id_V$$

Proof. Since $\mathcal{C}_\mathsf{k}(G) = Z(\mathsf{k}[G])$ the endomorphism $\rho(f)$ commutes with the action of G, and hence by Schur's lemma $\rho(f)$ is $\lambda.\mathrm{id}_V$ for some $\lambda \in \mathsf{k}$. To calculate the scalar λ note that $\mathrm{tr}(\lambda.\mathrm{id}_V) = \lambda.\dim(V)$, hence we see that

$$\begin{aligned}\lambda &= \frac{1}{\dim(V)} \sum_{g \in G} f(g)\mathrm{tr}(\rho(g)) \\ &= \frac{|G|}{\dim(V)} \langle f, \chi_V^* \rangle.\end{aligned}$$

□

Definition 4.10. For V be an irreducible representation let

$$c_V = \frac{\dim(V)}{|G|} \sum_{g \in G} \chi_V(g^{-1}) e_g \in \mathsf{k}[G].$$

Since χ_V is a class function, so is c_V, indeed $c_V = \frac{\dim(V)}{|G|} \chi_V^*$.

Notice that if V is the trivial representation, then c_V is just the element I_G we studied earlier. Moreover Lemma 4.9 and Theorem 4.5 immediately show the following:

Lemma 4.11. *Let (W, ρ) be a representation of G, and let $W = \bigoplus_{j \in J} W^j$ be its isotypical decomposition. Then $\rho(c_V)$ is the projection to the isotypical summand corresponding to V.*

Proof. It is enough to show that $\rho(c_V)$ restricts to the identity on any irreducible summand of W isomorphic to V, and to zero on any irreducible summand of W not isomorphic to V. But by Lemma 4.9 $\rho(c_V)$ acts on W by the scalar

$$\frac{\dim(V)}{\dim(W)}\langle \chi_V^*, \chi_W^*\rangle,$$

which by Theorem 4.5 is clearly 1 if $V \cong W$ and 0 otherwise. □

Let $\{U_j : j \in J\}$ be a complete set of representatives for the irreducible representations of G, and let $\chi_j = \chi_{U_j}$ and $c_j := c_{U_j} = \frac{\dim(U_j)}{|G|}\chi_j^*$. It follows from the above that given any representation (W, ρ) of G, we have

$$\sum_{j\in J}\rho(c_j) = 1, \quad \rho(c_j)^2 = \rho(c_j), \quad \rho(c_j)\rho(c_k) = 0 \text{ if } j \neq k.$$

Proposition 4.12. *The set $\{c_j : j \in J\}$ is a basis for the space of class functions $\mathcal{C}_{\mathsf{k}}(G)$. Thus the number of irreducible representations is equal to the number of conjugacy classes in G. Moreover the character $\{\chi_j : j \in J\}$ also form a basis for the space of class functions.*

Proof. Let $z \in \mathcal{C}_{\mathsf{k}}(G)$. Now z acts by the scalar $\lambda_j = \frac{|G|}{\dim(U_j)}\langle z, \chi_j^*\rangle$ on U_j. Thus it follows $\sum_{j\in J}\lambda_j c_j$ acts as z on any representation of G. Now considering the action of z on the unit e_e in the regular representation $\mathsf{k}[G]$ we see that

$$z = z \star e_e = \sum_{j\in J}\lambda_j c_j \star e_e = \sum_{j\in J}\lambda_j c_j.$$

Thus $\{c_j : j \in J\}$ spans the space $\mathcal{C}_{\mathsf{k}}(G)$. On the other hand, c_j is a nonzero multiple of χ_j^* for all $j \in J$, hence since the χ_j are linearly independent, the c_j must be also. Thus $\{c_j : j \in J\}$ is a basis for $\mathcal{C}_{\mathsf{k}}(G)$ (and hence $\{\chi_j : j \in J\}$ is also).

Since we have already seen that $\dim(\mathcal{C}_{\mathsf{k}}(G))$ is just the number of conjugacy classes in G, the proof is complete. □

Remark 4.13. When we work over $\mathbb{C}$ it is common to use, instead of $\langle -, -\rangle$, the Hermitian form

$$(f, g) = |G|^{-1}\sum_{k\in G} f(k)\overline{g(k)}$$

Since over the complex numbers $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ the above proofs show that over $\mathbb{C}$, the characters of irreducible representations form an orthonormal basis of the space $\mathcal{C}_{\mathbb{C}}(G)$.

We finish this section with a description of the regular representation. The character of the regular representation is easy to compute. Indeed using the basis $\{e_g : g \in G\}$ we see that $\mathrm{tr}(g, \mathsf{k}[G])$ is zero unless $g = e$ (since the matrix corresponding to g in this basis will consist of 1s and 0s with a 1 in the diagonal exactly when $gh = h$, that is when $g = e$). Thus

$$\chi_{\mathsf{k}[G]}(g) = \begin{cases} |G|, & \text{if } g = e, \\ 0, & \text{otherwise.}\end{cases}$$

It follows from this, and the fact that $\chi_V(e) = \dim(V)$ for every representation V, that

$$\dim(\mathrm{Hom}_G(\mathsf{k}[G], V)) = \langle \chi_{\mathsf{k}[G]}, \chi_V\rangle = \dim(V).$$

Now suppose that $V = U_j$. Then the dimension of this space is the number of times that U_j occurs in $\mathsf{k}[G]$, and so we see that

$$\mathsf{k}[G] \cong \bigoplus_{j \in J} U_j^{\oplus \dim(U_j)}.$$

as G-representations, and hence

$$|G| = \sum_{j \in J} \dim(U_j)^2 \tag{4.2}$$

Theorem 4.14 (Wedderburn)**.** *Let $\{U_j : j \in J\}$ be a complete set of irreducible representations of G. Then there is a natural isomophism*

$$\theta \colon \mathsf{k}[G] \to \bigoplus_{j \in J} \mathit{End}_{\mathsf{k}}(U_j).$$

Proof. Since each U_j is a G-representation, there is a natural map

$$\theta_j \colon \mathsf{k}[G] \to \mathrm{End}_{\mathsf{k}}(U_j).$$

Let θ be the direct sum of these maps. Now since Equation 4.2 shows that the two algebras $\mathsf{k}[G]$ and $\bigoplus_{j \in J} \mathrm{End}_{\mathsf{k}}(U_j)$ have the same dimension, it is enough to show that θ is injective. But if $f \in \mathsf{k}[G]$ has $\theta(f) = 0$, then f acts as zero on any irreducible representation of G, and hence on any representation of G, and in particular is zero on the regular representation $\mathsf{k}[G]$. But then $f = f \star e_e = 0$, and we are done. $\square$

LINEAR REPRESENTATIONS: SCHURS' LEMMA AND CHARACTER THEORY

KEVIN MCGERTY

We have now established that any representation is a direct sum of irreducible representations, so that in order to classify representations, it is enough to classify the irreducible ones. (This is much the same as the way we were able to reduce the classification of G-sets to the classification of transitive G-sets.) In this section we study irreducible representations, by considering the space of G-equivariant maps between them. As a consequence, for example, we will be able to give a criterion to check if a given representation is irreducible. (Recall in the previous section we decomposed the natural permutation representation of S_n into two pieces, one of which was irreducible, but we did not established the same property for the other summand.)

Another question we will address is uniqueness: we have shown that any representation V of a finite group G over $\mathbb{C}$ is a direct sum of irreducible subrepresentations. To what extent is the decomposition of V into irreducible summands unique? Already just by considering the direct sum of two copies of the trivial representation of G, we see that there cannot be uniqueness in general, but we will obtain a somewhat weaker statement: a slightly coarser decomposition of V into *isotypical* subrepresentations *is* unique. This will also imply that the the decomposition of V into irreducibles is unique up to isomorphism.

1. SCHUR'S LEMMA

In this section k *is an arbitrary field unless otherwise stated.*

We begin with a following lemma which, while very easy to prove, is of fundamental importance.

Lemma 1.1 (Schur). *Let V and W be representations of G, and suppose that $\phi\colon V \to W$ is a G-equivariant map. Then if V is irreducible, ϕ is either zero or injective, while if W is irreducible, then ϕ is either zero or surjective. In particular, if V and W are both irreducible then ϕ is either zero or an isomorphism.*

Proof. The subspace $\ker(\phi)$ is a G-subrepresentation of V: indeed if $\phi(v) = 0$, then $\phi(g(v)) = g(\phi(v)) = 0$, so that $g(v) \in \ker(\phi)$. Similarly $\mathrm{im}(\phi)$ is a G-subrepresentation of W. If V is irreducible the $\ker(\phi)$ must either be $\{0\}$ or all of V, hence ϕ is injective or zero. In the same way, if W is irreducible then $\mathrm{im}(\phi)$ is either $\{0\}$ or all of W, so that ϕ is zero or surjective. $\square$

An easy consequence of this (which is sometimes also called Schur's Lemma) is the following result. Recall that for G-representations V, W. we write $\mathrm{Hom}_G(V, W)$ is the space of G-equivariant linear maps from V to W. If $V = W$ we may also write $\mathrm{End}_G(V)$.

Date: January 2009.

Corollary 1.2. *Suppose that* k *is an algebraically closed field. Then if* V *is an irreducible* G*-representation* $End_G(V) = \mathsf{k}$*. Moreover if* V *and* W *are irreducible representations then* $Hom_G(V, W)$ *is either zero or one-dimensional.*

Proof. Suppose that $\phi \in \mathrm{End}_G(V)$. Then since k is algebraically closed, ϕ has an eigenvector λ say. But then $\phi - \lambda \in \mathrm{End}_G(V)$, and has a non-trivial kernel, so in particular it is not an isomorphism. But then by Schur's lemma, it must be zero, that is $\phi = \lambda$ as claimed.

To see the last part, note that if V and W are not isomorphic, Schur's lemma shows that $\mathrm{Hom}_G(V, W) = 0$. On the other hand, if $V \cong W$, then picking $\phi \in \mathrm{Hom}_G(V, W)$, we see that $\alpha \mapsto \phi^{-1} \circ \alpha$ gives and isomorphism between $\mathrm{Hom}_G(V, W)$ and $\mathrm{End}_G(V)$, which hence $\mathrm{Hom}_G(V, W)$ is one-dimensional as required. ☐

Note that if k is not algebraically closed, then all we can conclude from Schur's lemma is that $\mathrm{End}_G(V)$ is a division algebra (or skew-field), that is, the nonzero elements of $\mathrm{End}_G(V)$ are all invertible (so that $\mathrm{End}_G(V)$ is like a field, except that the multiplication is not necessarily commutative).

Example 1.3. Suppose that $G = \mathbb{Z}/3\mathbb{Z}$ is the cyclic group of order 3. Then $\rho(1) = R$ where

$$R = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

(the matrix of rotation by $2\pi/3$ about 0) defines a representation of G on $\mathbb{R}^2$ which is irreducible (over $\mathbb{R}$). It is easy to see that $\mathrm{End}_G(\mathbb{R}^2) \cong \mathbb{C}$ in this case. Since we are primarily interested in the case $\mathsf{k} = \mathbb{C}$, we will mostly just assume that k is algebraically closed.

To show how useful Schur's lemma is, we now use it to describe the representations of Abelian groups in ordinary characteristic (over an algebraically closed field). We already know that any representation is completely reducible, so that it is enough to understand the irreducible representations.

Lemma 1.4. *Suppose that* k *is algebraically closed, and* G *is an Abelian group. If* (V, α) *is an irreducible representation of* G *then* V *is one-dimensional.*

Proof. Let $g \in G$. Since G is Abelian, $\alpha(g)$ commutes with $\alpha(h)$ for all $h \in G$, and so $\alpha(g) \in \mathrm{End}_G(V)$. But then by the corollary to Schur's lemma, $\alpha(g)$ is a scalar. Since g was arbitrary, we see that $\alpha(g) \in \mathsf{k}$ for all $g \in G$, and hence since V is irreducible, V must have dimension 1 as required. ☐

Note that our previous example shows that this result is false if we do not assume k is algebraically closed. If G is a cyclic group $\mathbb{Z}/n\mathbb{Z}$, then the one-dimensional representations of G are given by picking a $\zeta \in \mathsf{k}$ such that $\zeta^n = 1$. Hence if k contains ζ a primitive n-th root of unity (for example $e^{2\pi i/n}$ when $\mathsf{k} = \mathbb{C}$), the irreducible representations of $\mathbb{Z}/n\mathbb{Z}$ are given by the set $\{\zeta^k : 1 \leq k \leq n\}$. Since any Abelian group can be written as a product of cyclic groups, say $G = \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$ we see that the irreducible G-representations are given by r-tuples $(\zeta_1^{i_1}, \ldots, \zeta_r^{i_r})$ where ζ_i is a primitive n_i-th root of unity, and $1 \leq i_j \leq n_j$. Thus we see there are exactly $|G|$ irreducible representations of an Abelian group G[1]. We summarize this in the following proposition.

Proposition 1.5. *Let G be a finite abelian group, and suppose that k is an algebraically closed field which is ordinary for G. Then all the irreducible representations of G are 1-dimensional, and there are $|G|$ distinct irreducible representations.*

The example of S_3 which we already worked out using just linear algebra shows that for non-Abelian groups the number of irreducible representations can be smaller than $|G|$ (indeed $|S_3| = 6$, whereas we found 3 irreducible representations). You might wish to take a guess at what the number of irreducible representations actually is...

As another application of the the rigidity of irreducible representations, we prove the converse to a result of the previous section: if V is a sum of irreducible representations then any subrepresentation has an G-invariant complement. (Of course this is Maschke's theorem in the case where the order of the group is invertible in the field we are working over, but the proof below does not assume that G is finite, or indeed anything about the field k, only that the representations in question are finite dimensional). The proof is not an application of Schur's lemma, but it uses the same circle of ideas.

Lemma 1.6. *Suppose that V is a sum of irreducible representations of G. Then any subrepresentation of V has a G-invariant complement.*

Proof. Suppose that W is a proper subrepresentation of V, and consider the set $\mathcal{S}$ of all subrepresentations U of V such that $W \cap U = \{0\}$, so that the sum $W + U$ is direct. Pick U of maximal dimension in $\mathcal{S}$ (possibly we have $\dim(U) = 0$). Then either $W \oplus U = V$, in which case we are done, or $W \oplus U = W'$ is a proper subspace of V. But in that case, it cannot be that every irreducible subrepresentation of V lies in W', since V is the direct sum of irreducible subrepresentations. Thus there must be some irreducible subrepresentation N with N not contained in W'. But then $N \cap W'$ is a proper subrepresentation of N, and hence by the irreducibility of N, it must be zero. Then the sum $W' + N$ is direct. But then

$$(W \oplus U) \oplus N = W \oplus (U \oplus N)$$

is a direct sum and $(U \oplus N)$ has strictly greater dimension than U, which contradicts the choice of U. $\square$

Remark 1.7. Note that we only assumed that V was a sum of irreducible representations, not a direct sum. Thus it actually follows from this Lemma and the proof that Maschke's theorem implies complete reducibility that if V is a sum of irreducible subrepresentations, then it must in fact be a direct sum of irreducible subrepresentations.

Next we use Schur's lemma to show that there are only finitely many isomorphism classes of irreducible representations of a finite group G. Recall that if X is a finite G-set, the space of functions on X is naturally a representation of G. Taking $X = G$ with the left action of G on itself, we see that $\mathbb{C}[G]$, the space of functions

[1] If k doesn't contain the appropriate primitive roots of unity, then this conclusion fails. If $\mathrm{char}(\mathsf{k}) = p$ and p divides n_i this always happens (as then $x^p - 1 = (x-1)^p$), so we see that it is not enough for k to be algebraically closed: the result only holds for ordinary fields for G.

on G is a representation of G. This is called the *regular representation*. It has a basis $\{e_h : h \in G\}$, and the action of G in terms of this basis is $g(e_h) = e_{gh}$, for $g, h \in G$.

Lemma 1.8. *Suppose that k is ordinary for G, and let V be an irreducible representation of G. Then V isomorphic to a subrepresentation of $\mathsf{k}[G]$.*

Proof. Pick a vector $v \in V$, and let $\phi\colon \mathsf{k}[G] \to V$ be given by $e_g \mapsto g(v)$. Then it is easy to see that this map is G-equivariant: indeed

$$\phi(g(e_h)) = \phi(e_{gh}) = (gh).v = g(h.v) = g(\phi(e_h)).$$

But since $\phi(e_e) = v$ we see that $\phi \neq 0$, so that as V is irreducible, Schur's lemma implies that ϕ is surjective. Now $\ker(\phi)$ is a subrepresentation of $\mathsf{k}[G]$, and so by Maschke's theorem it has a G-invariant complement U in $\mathsf{k}[G]$. But then ϕ induces an isomorphism from U to V, and we are done. $\square$

Remark 1.9. Notice that this gives a concrete bound of at most $|G|$ irreducible representations, which is exactly what we saw for Abelian groups. Moreover we now see that to understand all the irreducible representations of G it is enough to decompose the regular representation into irreducibles.

Remark 1.10. If k is an arbitrary field, not necessarily ordinary for G (or indeed even algebraically closed), then the previous theorem still shows that any irreducible representation is a quotient of $\mathsf{k}[G]$.

2. Homomorphisms and the isotypical decomposition

In this section we assume that k is algebraically closed and ordinary for G.

We can now also establish a decomposition of any representation into summands which are canonical. Take a set of irreducible representations $\{U_j : j \in J\}$ such that any irreducible is isomorphic to exactly one U_j (so that by what we have just shown, J is a finite set).

Now suppose that V is a representation of G. Then we may decompose $V = \bigoplus_{i=1}^n V_i$ into a direct sum of irreducible representations (not necessarily in a unique way). For each $j \in J$ let $V^j = \bigoplus V_i$ where the sum is over the V_i such that $V_i \cong U_j$. The decomposition $V = \bigoplus_{j \in J} V^j$ is known as an *isotypical decomposition* of V. It is unique, whereas the decomposition $V = \bigoplus_i V_i$ into irreducible subrepresentations is not.

Lemma 2.1. *Let V and W be representations of G, and suppose that $\bigoplus_j V^j$ and $\bigoplus_j W^j$ are isotypical decompositions of V and W respectively. Then if $\phi \in \mathrm{Hom}_G(V, W)$ we have $\phi(V_j) \subseteq W_j$. In particular, the isotypical decomposition is unique.*

Proof. For $k \in J$ let $\iota_k\colon V^k \to V$ be the inclusion of V^k into V, and similarly let $\pi_l\colon W \to W^l$ be the projection from W to the l-th summand W^l. Given $\phi \in \mathrm{Hom}_G(V, W)$ let $\phi_{kl}\colon V^k \to W^l$ be the map $\pi_l \circ \phi \circ \iota_k$. Thus $(\phi_{kl})_{k,l \in J}$ is the "block matrix" decomposition of ϕ according to the isotypic summands V_k and W_l.

Decomposing (arbitrarily) each V_k and W_l into irreducible subrepresentations, and then using Schur's lemma we immediately see that $\phi_{kl} = 0$ when $k \neq l$, and so $\phi(V^j) \subset W^j$ as required. To see that this implies the isotypical decomposition is unique, apply the first part of the lemma to the identity map $\mathrm{id}\colon V \to V$. $\square$

Remark 2.2. Note that while the decomposition of V into irreducible subrepresentations is not unique, the decomposition of V into irreducibles is unique *up to isomorphism*, since the decomposition $V = \bigoplus_{j \in J} V^j$ is unique, and we have $V^j \cong U_j^{\oplus d_j}$ where d_j can be calculated from the dimension of V^j, indeed $d_j = \dim(V^j)/\dim(U_j)$.

Example 2.3. Recall our description of the representations of

$$S_3 = \langle s, t : s^2 = t^3 = 1, sts^{-1} = t^{-1} \rangle.$$

over a field k of characteristic greater than 3. A representation of S_3 on a vector space V is given by a pair of linear maps S, T satisfying the relations $S^2 = T^3 = \mathrm{Id}_V$ and $STS^{-1} = T^{-1}$, and we can decompose V according to the eigenvalues of the matrices S and T (the linear maps S and T are diagonalizable since char$(\mathsf{k}) \neq 2, 3$). Indeed taking ω a primitive 3rd root of unity, we set

$$\begin{aligned} W_1 &= \{v \in V : S(v) = T(v) = v\}, \quad W_{-1} = \{v \in V : S(v) = v, T(v) = -v\}, \\ V_{\omega^{\pm 1}} &= \{v \in V : T(v) = \omega^{\pm 1} v\}. \end{aligned}$$

Each of these subspaces is a subrepresentation, and they give the isotypical decomposition of V: the subrepresentation W_1 is the direct sum of copies of the trivial representation, the subrepresentation W_{-1} is a direct sum of the one-dimensional representation where s acts as -1 and t acts as 1, while $V_{\omega^{\pm 1}}$ is a direct sum of copies of the irreducible two-dimensional representation.

Note that while the decomposition of V into these three subspaces involves no choices, to decompose V further into irreducible subrepresentations we must choose an arbitrary decomposition of W_1 and W_{-1} into one-dimensional subspaces and $V_{\omega^{\pm 1}}$ into 2-dimensional subrepresentations (which can be done as we did previously by choosing a basis of the ω-eigenspace of T). On the other hand, given any two such choices of a decomposition, we can find a G-equivariant isomorphism of V to itself which interchanges them, which verifies that the decomposition of V into irreducibles is unique up to isomorphism.

Schur's lemma in fact gives us a complete description of what the space of equivariant homomorphisms between two G-representations looks like. Indeed by the previous lemma on the isotypic decomposition, we need only consider representations which are isotypic, and the next lemma deals with this case.

Lemma 2.4. *Let $V \cong U^{\oplus n}$ and $W \cong U^{\oplus m}$ be G-representations, where U is irreducible. Then*

$$Hom_G(V, W) \cong Mat_{n,m}(\mathsf{k}).$$

Proof. We use a block matrix decomposition again. Let $V = \bigoplus_{i=1}^n V_i$ where $V_i \cong U$ for all i, and similarly $W = \bigoplus_{j=1}^m W_j$ with $W_j \cong U$ for all j. Then for i, j with $1 \leq i \leq n$ let $\iota_i \colon V_i \to V$ be the inclusion of V_i into V as the i-th term of the direct sum, and let $\pi_j \colon W \to W_j$ be the projection from W to the j-th summand W_j. Given $\phi \in \mathrm{Hom}_G(V, W)$ let $\phi_{ij} \colon V_i \to W_j$ be the map $\pi_j \circ \phi \circ \iota_i$. If we fix an isomorphism $V_i \cong U$ and $W_j \cong U$ for each i, j, then we obtain isomorphisms $\mathrm{Hom}_G(V_i, W_j) \cong \mathrm{Hom}_G(U, U = \mathsf{k}$, where the last equality follows from Schur's lemma. Hence we may identify each ϕ_{ij} with a scalar, λ_{ij} say. Then the map $\phi \mapsto (\lambda_{ij})$ gives the required isomorphism. $\square$

Remark 2.5. Note that the isomorphism given in the previous lemma is not unique, in the same way that if V and W are vector spaces of dimension n and m respectively, then $\mathrm{Hom}(V, W)$ is isomorphic to $\mathrm{Mat}_{n,m}(\mathsf{k})$, but one must pick bases of V and W in order to define an isomorphism.

Let us put the two previous lemmas together to give an explicit description of $\mathrm{Hom}_G(V, W)$ for two arbitrary representations of G.

Proposition 2.6. *Let V and W be linear representations of G, and let $V = \bigoplus_{j\in J} V^j$, and $W = \bigoplus_{j\in J} W^j$ be their isotypical decompositions. Then if $V^j \cong U_j^{\oplus n_j}$ and $W^j \cong U_j^{\oplus m_j}$ for integers $n_j, m_j, (j \in J)$ we have*

$$Hom_G(V, W) \cong \bigoplus_{j\in J} Mat_{n_j,m_j}(\mathsf{k}).$$

Proof. By Lemma 2.1 we see immediately that

$$\mathrm{Hom}_G(V, W) = \bigoplus_{j\in J} \mathrm{Hom}_G(V^j, W^j),$$

and then using Lemma 2.4 we see that the j-th term in this sum is isomorphic to $\mathrm{Mat}_{n_j,m_j}(\mathsf{k})$ as required. □

Now let's extract some numerical information from this. Let $V \cong \bigoplus_{j\in J} U_j^{\oplus n_j}$. Taking $V = W$ in the Proposition 2.6 it ifollows immediately that

$$\dim(\mathrm{Hom}_G(V, V)) = \sum_{j\in J} n_j^2. \tag{2.1}$$

We can use this to give a numerical criterion for a representation to be irreducible.

Corollary 2.7. *Suppose that V is a representation of G. Then V is irreducible if and only if*

$$\dim(Hom_G(V, V)) = 1.$$

Proof. We use the notation of the previous paragraph. Equation 2.1 shows that the dimension of $\mathrm{Hom}_G(V, V)$ is $\sum_{j\in J} n_j^2$. Such a sum of squares is equal to 1 if and only if exactly one of the n_js is 1 and all the rest are zero, that is, when V is irreducible. □

Recall that if V and W are G-representations, then $\mathrm{Hom}(V, W)$, the space of all linear maps from V to W, is a G-representation, and moreover, the space of G-equivariant linear maps $\mathrm{Hom}_G(V, W)$ is just the subspace of $\mathrm{Hom}(V, W)$ on which G acts trivially. Thus rephrasing our condition above, we see that to show that a representation V is irreducible, we need only show that the trivial representation occurs exactly once in $\mathrm{Hom}(V, V)$.

Definition 2.8. Let (V, ρ) be a G-representation. Then the subspace

$$V^G = \{v \in V : \rho(g)(v) = v, \forall g \in G\},$$

is the isotypic summand corresponding to the trivial representation. It is known as the space of G-invariants in V. If V, W are G-representations, then $\mathrm{Hom}_G(V, W)$ is by definition $\mathrm{Hom}(V, W)^G$.

Although we now have a numerical criterion for irreducibility, it is not yet clear that it is a particularly useful or computable one. In fact an idea we have already used in the proof of Maschke's lemma will allows us to turn this criterion into a very computable one. Recall that the key to that proof was to average an arbitrary projection to obtain a G-equivariant one. We now formalize this averaging trick using $\mathbb{C}[G]$, the space of complex-valued functions on G. Thus we take a short detour to study the properties of $\mathbb{C}[G]$.

3. THE GROUP ALGEBRA

In this section we assume that k *is ordinary for* G*, that is* k *is algebraically closed and* $|G|$ *is invertible in* k*.*

The vector space $\mathsf{k}[G]$ of functions on G has more structure that just a linear action of G.

Definition 3.1. A k-algebra is a (not necessarily commutative) ring A which contains k as a central commutative subring, so that $\lambda.x = x.\lambda$ for all $x \in A, \lambda \in \mathsf{k}$. Thus in particular A is a k-vector space. Given two k-algebras A and B, a homomorphism of k-algebras is a k-linear map $\alpha\colon A \to B$ which respects multiplication and maps the identity element in A to that in B, that is,

$$\alpha(x.y) = \alpha(x).\alpha(y), \quad \forall x, y \in A; \quad \alpha(1_A) = 1_B.$$

Example 3.2. Let V be a k-vector space. Then the space $\mathrm{End}_{\mathsf{k}}(V)$ of linear maps from V to itself is a k-algebra.

We can make $\mathbb{C}[G]$ into a k-algebra using a *convolution product*[2]: namely we may define $\star\colon \mathbb{C}[G] \times \mathbb{C}[G] \to \mathbb{C}[G]$ by

$$(f \star g)(k) = \sum_{h \in G} f(kh^{-1}).g(h),$$

for any $k \in G$. More concretely, using the basis $\{e_g : g \in G\}$ of indicator functions, you can check that

$$e_g \star e_h = e_{gh}, \quad \forall g, h \in G \tag{3.1}$$

Thus e_e the indicator function of the identity element of G is the unit in $\mathsf{k}[G]$, so that the field k is embedded in $\mathsf{k}[G]$ by the map $\lambda \mapsto \lambda e_e$.

Given a representation (V, ρ) of G, we can extend ρ to a map, which we also write as ρ, from $\mathsf{k}[G] \to \mathrm{End}(V)$ given by

$$f \mapsto \sum_{g \in G} f(g)\rho(g).$$

It follows from Equation 3.1 that $\rho\colon \mathsf{k}[G] \to \mathrm{End}(V)$ is a map of k-algebras, that is

$$\rho(f \star g) = \rho(f) \circ \rho(g),$$

where on the right-hand side $\circ$ denotes composition of endomorphisms. In fact we can reformulate the study of G-representations in terms of the group algebra.

Lemma 3.3. *Let V be a* k*-vector space. Then giving a linear action of G on V is equivalent to giving an algebra map* $\mathsf{k}[G] \to$ *End*(V)*.*

[2] You should compare this to the convolution product of functions you may have seen in Fourier theory: for f, g functions on $\mathbb{R}$, the convolution of f with g is $(f \star g)(x) = \int f(x-y)g(y)dy$.

Proof. We have already seen that given $\rho\colon G \to \mathrm{GL}(V)$, we may construct an algebra map from $\mathsf{k}[G] \to \mathrm{End}(V)$. Thus we need only check the converse. Suppose that $\rho\colon \mathsf{k}[G] \to \mathrm{End}(V)$. For $g \in G$ set $\rho_G(g) = \rho(e_g)$. Then since $\rho(e_g \star e_h) = \rho(e_g) \circ \rho(e_h)$ we see that

$$\rho_G(g.h) = \rho(e_{gh}) = \rho(e_g) \circ \rho(e_h) = \rho_G(g) \circ \rho_G(h).$$

But now since $\rho(e_e) = \mathrm{id}_V$, it follows that $\rho_G(g)$ is invertible for every $g \in G$ with inverse $\rho_G(g^{-1})$, and hence ρ_G is a homomorphism from G to $\mathrm{GL}(V)$ as required. □

We now use the group algebra to reformulate the averaging trick we used in the proof of Maschke's theorem. Let $I_G = |G|^{-1} \sum_{g\in G} e_g$, that is I_G is the function in $\mathbb{C}[G]$ which is equal to $|G|^{-1}$ on every point of G (thus we are assuming that $|G| \neq 0$ in k).

Lemma 3.4. *For any $g \in G$ we have $e_g \star I_G = I_G$, and hence $I_G^2 = I_G$. Moreover, if V is a G-representation, then $\rho(I_G)$ is the G-equivariant projection to the subspace V^G of V on which G acts trivially.*

Proof. We have

$$e_g \star I_G = e_g \star (|G|^{-1} \sum_{h\in G} e_h) = |G|^{-1} \sum_{h\in G} e_{gh} = |G|^{-1} \sum_{k\in G} e_k = I_G.$$

where $k = gh$ runs over all of G as h does. It is then clear that

$$I_G^2 = |G|^{-1}(\sum_{g\in G} e_g \star I_G) = |G|^{-1} \sum_{g\in G} I_G = I_G.$$

Now if (V, ρ) is a G-representation, it follows immediately that $\rho(I_G)$ is a projection operator (as $\rho(I_G)^2 = \rho(I_G^2) = \rho(I_G)$). Moreover, since $\rho(g) \circ \rho(I_G) = \rho(I_G)$ it is clear that G acts trivially on the image of $\rho(I_G)$, and also by the definition of I_G, if $\rho(g)(v) = v$ for all $g \in G$, then $\rho(I_G)(v) = v$. Thus $\rho(I_G)$ is the required projection. □

Remark 3.5. In the language we have just built up, our proof of Maschke's theorem took an arbitrary projection from V to the subrepresentation W and applied I_G to it (as an element of the representation $\mathrm{Hom}(V, V)$) to get an equivariant projection.

We are now finally able to make our irreducibility criterion more explicit: given a representation V, we wish to calculate $\dim(\mathrm{Hom}_G(V, V))$. By what we have shown above is that this dimension is just the rank of the projection operator I_G on the representation $\mathrm{Hom}(V, V)$. But the rank of a projection map is simply its trace, so that we find

$$\dim(\mathrm{Hom}_G(V, V)) = \mathrm{tr}(I_G, \mathrm{Hom}(V, V)).$$

Moreover, since trace is linear, it follows that

$$\dim(\mathrm{Hom}_G(V, V)) = |G|^{-1} \sum_{g\in G} \mathrm{tr}(g, \mathrm{Hom}(V, V)).$$

We summarize the above into the following proposition.

Proposition 3.6. *Let (V, ρ) be a G-representation. Then*

$$\dim(Hom_G(V,V)) = |G|^{-1} \sum_{g \in G} tr(g, Hom(V,V)),$$

thus in particular V is irreducible if and only if

$$|G|^{-1} \sum_{g \in G} tr(g, Hom(V,V)) = 1$$

Example 3.7. Consider the symmetric group S_n and the set $X = \{1, 2, \ldots, n\}$ on which it acts. We already decomposed the permutation representation $\mathbb{C}[X]$ into two pieces:

$$\mathbb{C}[X] = \mathbb{C}\langle v \rangle \oplus \{f \in \mathbb{C}[X] : \sum_{1 \leq i \leq n} f(i) = 0\}.$$

where $v = \sum_{i=1}^{n} e_i$. We are now able to show that this decomposition is in fact into irreducible subrepresentations.

Indeed these are distinct irreducible representations if and only if

$$\dim(\mathrm{Hom}_G(\mathbb{C}[X], \mathbb{C}[X])) = 2.$$

To calculate $\dim(\mathrm{Hom}_G(\mathbb{C}[X], \mathbb{C}[X]))$ we need only calculate the sum of the traces $\mathrm{tr}(g, \mathrm{Hom}(\mathbb{C}[X], \mathbb{C}[X]))$ for each $g \in S_n$. Let $\{e_i : 1 \leq i \leq n\}$ be the basis of indicator functions for $\mathbb{C}[X]$. Then we can define a natural basis $\{e_{ij} : 1 \leq i, j \leq n\}$ of $\mathrm{Hom}(\mathbb{C}[X], \mathbb{C}[X])$ in terms of this basis, such that $e_{ij}(e_k) = e_j$ if $k = i$ and zero otherwise. It is easy to check that $g(e_{ij}) = e_{g(i),g(j))}$.

It follows from this that if we calculate the trace of $g \in S_n$ on the basis $\{e_{ij} : 1 \leq i, j \leq n\}$ then

$$\mathrm{tr}(g, \mathrm{Hom}(V,V)) = |\{(i,j) : 1 \leq i, j \leq n, g(i) = i, g(j) = j\}|,$$

since the diagonal entry $((ij), (ij))$ will be zero or 1 according to whether $g(i) = i$ and $g(j) = j$ or not. Hence

$$\dim(\mathrm{Hom}_G(V,V)) = |G|^{-1} \sum_{g \in G} F_{X \times X}(g),$$

where $F_{X \times X}(g)$ is the number of fixed points of S_n on the set $X \times X$. But now Burnsides theorem says that this is just the number of orbits of S_n on $X \times X$. But this is clearly 2: the pairs $\{(i,i) : 1 \leq i \leq n\}$ form one orbit, while the pairs $\{(i,j) : i \neq j\}$ form the other.

4. Character Theory

In this section k *is assumed to be ordinary for G.*

Given a linear map $\alpha \colon V \to V$, there are a number of natural invariants associated to it: we may take its trace, its determinant, or perhaps most comprehensively its characteristic polynomial $\det(\lambda - \alpha)$. Thus given a group G acting linearly on V, we can attach to it these invariants for each group element. Since $\det \colon \mathrm{GL}(V) \to \mathsf{k}^\times = \mathrm{GL}_1(\mathsf{k})$ is a group homomorphism, the determinant map actually yields a new one-dimensional representation of G. However, since for example any perfect group[3] has no nontrivial one-dimensional representations we

[3]*i.e.* a group for which G which is equal to its own derived group $[G, G]$, which is the case for every non-Abelian simple group.

cannot expect that this will record much information about our original representation V. On the other hand, we have already seen in the last section that knowing traces of the elements of G (admittedly on $\text{Hom}(V, V)$ not V) allows us to test if V is irreducible. In fact with not much more work we will be able to see that the traces yield a complete invariant of V.

Definition 4.1. Let (V, ρ) be a representation of G. Then the character of V is the k-valued function

$$\chi_V : G \to \mathsf{k}, \quad \chi_V(g) = \text{tr}(\rho(g)).$$

Lemma 4.2. *Suppose that (V, ρ) is a representation of G. Then*

(1) *If $g \in G$ then $\rho(g)$ is diagonalizable. If $\mathsf{k} = \mathbb{C}$ then $\chi_V(g^{-1}) = \overline{\chi_V(g)}$, where the bar denotes complex conjugation.*
(2) $\chi_V(e) = \dim(V)$.
(3) *χ_V is conjugation-invariant, that is $\chi_V(ghg^{-1}) = \chi_V(h)$ for all $g, h \in G$.*
(4) *If V^* is the dual representation, then $\chi_{V^*}(g) = \chi_V(g^{-1})$.*
(5) *If V and W are G-representations then $\chi_{V \oplus W} = \chi_V + \chi_W$.*

Proof. Let $C = \langle g \rangle$ be the subgroup of G generated by g. It is clear that C, the group generated by g, is a finite cyclic subgroup of G, hence we see that as a C-representation, V splits as a direct sum of lines. Since $g \in C$ we immediately see that g is diagonalizable as required. Picking a basis $\{e_1, e_2, \ldots, e_n\}$ of eigenvectors of g, so that $g(e_i) = \lambda_i e_i$ say, we have $\chi_V(g) = \sum_{i=1}^n \lambda_i$. Since $\rho(g^{-1}) = \rho(g)^{-1}$ is diagonal on the same basis, with eigenvalues λ_i^{-1}, it follows $\chi_V(g^{-1}) = \sum_{i=1}^n \lambda_i^{-1}$. If $\mathsf{k} = \mathbb{C}$, then since $\rho(g)^{|G|} = \text{id}$ for any $g \in G$, the eigenvalues of $\rho(g)$ are roots of unity, and hence they have modulus 1. But if $z \in \mathbb{C}$ has $|z| = 1$ then $z^{-1} = \bar{z}$, and since complex conjugation is linear, it follows that $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

The second part is clear, since $\rho(e) = \text{id}_V$ and the trace of the identity endomorphism is clearly just the dimension of V. For the third part, if $g, h \in G$ then

$$\chi_V(ghg^{-1}) = \text{tr}(\rho(ghg^{-1})) = \text{tr}(\rho(g)\rho(h)\rho(g)^{-1}) = \text{tr}(\rho(h)) = \chi_V(h).$$

since $\text{tr}(\alpha\beta) = \text{tr}(\beta\alpha)$ for all $\alpha, \beta \in \text{End}(V)$.

For the fourth part suppose $\alpha : V \to V$ is a linear map. If A is the matrix of α with respect to some basis of V, then the matrix of α^t with respect to the corresponding dual basis of V^* is A^t. But clearly $\text{tr}(A) = \text{tr}(A^t)$, so $\text{tr}(\alpha) = \text{tr}(\alpha^t)$. Now if $g \in G$, then $\rho^*(g) = \rho(g^{-1})^t$, hence we see

$$\chi_{V^*}(g) = \text{tr}(\rho(g^{-1})^t) = \text{tr}(\rho(g^{-1})) = \chi_V(g^{-1}),$$

as claimed.

Finally, if $U = V \oplus W$ and $\alpha : U \to U$ preserves each of V and W, then picking a basis of V and a basis of W their union is a basis of U with see that with respect to this basis the matrix of α has the form

$$\left(\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}\right)$$

Thus clearly $\text{tr}(\alpha) = \text{tr}(\alpha_{|V}) + \text{tr}(\alpha_{|W})$. Applying this observation to each $\rho(g)$ part four is now clear. $\square$

Definition 4.3. A function $f \in \mathsf{k}[G]$ is said to be a *class function* if $f(ghg^{-1}) = f(h)$, that is, if f is constant on the conjugacy classes of G. Let $\mathcal{C}_{\mathsf{k}}(G)$ denote the space of class functions on G. The space $\mathcal{C}_{\mathsf{k}}(G)$ has an obvious basis: for a conjugacy class

$\mathcal{C} \subseteq G$ let $z_{\mathcal{C}}$ be the indicator function of $\mathcal{C}$, so that $z_{\mathcal{C}} = \sum_{g \in \mathcal{C}} e_g$. Clearly the set $\{z_{\mathcal{C}} : \mathcal{C} \text{ a conjugacy class of } G\}$ is a basis of $\mathcal{C}_{\mathsf{k}}(G)$. Thus

$$\dim(\mathcal{C}_{\mathsf{k}}(G)) = |\{\mathcal{C} : \mathcal{C} \subseteq G \text{ a conjugacy class}\}|$$

The previous lemma shows that if V is a representation, then χ_V is a class function on G, thus at first sight it might seem to hold rather little information. However our study of G-equivariant maps between representations in terms of the element $I_G \in \mathsf{k}[G]$ suggests otherwise. Indeed if V and W are representations, then we have

$$\begin{aligned} \dim(\mathrm{Hom}_G(V,W)) &= \dim(\mathrm{Hom}(V,W)^G) \\ &= \mathrm{tr}(I_G, \mathrm{Hom}(V,W)) \\ &= |G|^{-1} \sum_{g \in G} \mathrm{tr}(g, \mathrm{Hom}(V,W)) \\ &= |G|^{-1} \sum_{g \in G} \chi_{\mathrm{Hom}(V,W)}(g). \end{aligned} \tag{4.1}$$

Thus if we can determine the character of $\mathrm{Hom}(V,W)$ in terms of that of V and W, we will be able to calculate the dimension of the space of equivariant maps between V and W.

Proposition 4.4. *Suppose that V and W are finite-dimensional G-representations. Then*

$$tr(g, Hom(V,W)) = \chi_V(g^{-1})\chi_W(g), \quad \forall g \in G.$$

Proof. Let $g \in G$. The action of g on V and W is diagonalizable, thus we may pick bases $\{e_1, e_2, \dots, e_n\}$ and $\{f_1, f_2, \dots, f_m\}$ of V and W respectively such that $g(e_i) = \lambda_i e_i$ and $g(w_j) = \mu_j w_j$ for some scalars $\lambda_i, \mu_j \in \mathsf{k}$. Calculating the trace of g^{-1} on V and g on W with respect to these bases we see

$$\chi_V(g^{-1}) = \sum_{1 \le i \le n} \lambda_i^{-1}, \quad \chi_W(g) = \sum_{1 \le j \le m} \mu_j.$$

Now $\mathrm{Hom}(V,W)$ has a basis $\{e_i^* f_j : 1 \le i \le n, 1 \le j \le m\}$, where $e_i^* f_j(v) = e_i^*(v) f_j$ for any $v \in V$. But $g(e_i^* f_j)(v) = e_i^*(g^{-1}(v)) g(f_j) = \lambda_i^{-1} \mu_j e_i^* f_j(v)$ for all $v \in V$, so that the functions $e_i^* f_j$ are eigenvectors for the action of g. Thus calculating the trace of g using this basis we see

$$\begin{aligned} \mathrm{tr}(g, \mathrm{Hom}(V,W)) &= \sum_{i,j} \lambda_i^{-1} \mu_j \\ &= (\sum_{1 \le i \le n} \lambda_i^{-1}).(\sum_{1 \le j \le m} \mu_j) \\ &= \chi_V(g^{-1})\chi_W(g). \end{aligned}$$

□

Motivated by this, we define a symmetric bilinear form on $\mathsf{k}[G]$. For $f \in \mathsf{k}[G]$ set $f^*(k) = f(k^{-1})$, and define

$$\begin{aligned} \langle f, g \rangle = |G|^{-1} \sum_{k \in G} f^*(k) g(k) &= |G|^{-1} \sum_{k \in G} f(k) g^*(k) \\ = |G|^{-1} \sum_{\substack{k_1, k_2 \in G \\ k_1.k_2 = 1}} f(k_1) g(k_2) &= |G|^{-1} (f \star g)(e). \end{aligned}$$

Note the map $f \mapsto f^*$ preserves the form $\langle -, - \rangle$ since $(f^*)^* = f$. The form $\langle -, - \rangle$ it is obviously nondegenerate since

$$\langle e_g, e_h \rangle = \begin{cases} |G|^{-1} & \text{if } g = h^{-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Equivalently $\{e_g : g \in G\}$ and $\{|G|e_g^* : g \in G\}$ are dual bases.

In fact it is the restriction of $\langle -, - \rangle$ to $\mathcal{C}_{\mathsf{k}}(G)$ which is most important for us. To better understand the form on $\mathcal{C}_{\mathsf{k}}(G)$, note that since conjugation is a group homomorphism, the inverse map induces a map on the set of conjugacy classes, and hence the map $f \mapsto f^*$ restricts to an endomorphism of $\mathcal{C}_{\mathsf{k}}(G)$. It is easy to see that

$$\langle z_{\mathcal{C}}, z_{\mathcal{D}} \rangle = \begin{cases} |\mathcal{C}|/|G|, & \text{if } z_{\mathcal{D}} = z_{\mathcal{C}}^*, \\ 0, & \text{otherwise.} \end{cases}$$

Thus $\langle -, - \rangle$ restricts to a nondegenerate symmetric form on $\mathcal{C}_{\mathsf{k}}(G)$ with $\{z_{\mathcal{C}}\}$ and $\{|\mathcal{C}|/|G|z_{\mathcal{C}}^*\}$ as dual bases.

Theorem 4.5. *Let V and W be representations of G with characters χ_V and χ_W respectively. Then*

$$\dim(Hom_G(V, W)) = \langle \chi_V, \chi_W \rangle.$$

In particular, if V and W are irreducible then

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

Proof. This is an immediate consequence of the previous lemma and Equation 4.1. □

This last theorem is remarkably powerful. We note now some of its important consequences.

Corollary 4.6. *Let $\{U_j : j \in J\}$ be a complete set of irreducible G-representations. Then the characters $\chi_j := \chi_{U_j} \in \mathcal{C}_{\mathsf{k}}(G)$ are linearly independent.*

Proof. Suppose that $\sum_{j \in J} a_j \chi_j = 0$ for some $a_j \in \mathsf{k}$. Then we have

$$0 = \langle \sum_{j \in J} a_j \chi_j, \chi_i \rangle = a_i,$$

for each $i \in J$. □

Notice that this gives a new bound on the number of irreducible representations: since the characters of nonisomorphic irreducible representations are linearly independent, their number is at most the dimension of $\mathcal{C}_{\mathsf{k}}(G)$, which is just the number of conjugacy classes in G. For non-Abelian groups G, this is an improvement on our earlier bound of $|G|$.

Corollary 4.7. *Let V be a G-representation. Then χ_V the character of V determines V up to isomorphism.*

Proof. If $\{U_j : j \in J\}$ is a complete set of irreducible G-representations, then by complete reducibility we know that $V \cong \bigoplus_{j \in J} U_j^{\oplus n_j}$. Thus V is determined up to isomorphism by the numbers $\{n_j : j \in J\}$. But we have already seen by our study of G-equivariant homomorphisms that

$$n_j = \dim(\mathrm{Hom}_G(V, U_j)),$$

and hence by Theorem 4.5 we have $n_j = \langle \chi_V, \chi_{U_j} \rangle$. $\square$

We now use character theory to give a more explicit description of the isotypical decomposition of a representation. Recall that $\mathsf{k}[G]$ is an algebra (the group algebra). The space of class functions has a natural description in terms of the algebra structure on $\mathsf{k}[G]$. If A is a k-algebra, we set

$$Z(A) = \{z \in A : xz = zx, \forall x \in A\}.$$

The set $Z(A)$ is called the *centre* of A. It is easy to check that $Z(A)$ is a (commutative) subalgebra of A.

Lemma 4.8. *The centre of the group algebra $\mathsf{k}[G]$ is the space of class functions $\mathcal{C}_{\mathsf{k}}(G)$.*

Proof. Recall that $\mathsf{k}[G]$ has a basis $\{e_g : g \in G\}$ and the multiplication in $\mathsf{k}[G]$ is given by $e_g.e_h = e_{gh}$. If $z = \sum_{k \in G} \lambda_k e_k$, then z is in $Z(A)$ if and only if we have $e_g.z = z.e_g$ for all $g \in G$. But since e_g is invertible with inverse $e_{g^{-1}}$ this is equivalent to the condition $e_g z e_{g^{-1}} = z$ for every $g \in G$. Now since $e_g e_k e_{g^{-1}} = e_{gkg^{-1}}$ this is equivalent to

$$\sum_{k \in G} \lambda_k e_{gkg^{-1}} = \sum_{k \in G} \lambda_k e_k, \quad \forall g \in G.$$

Thus $z \in Z(A)$ if and only if $\lambda_k = \lambda_{gkg^{-1}}$ for all $g \in G$, that is, if and only if z is a class function. $\square$

Lemma 4.9. *Let (V, ρ) be an irreducible representation of G, and let $f \in \mathcal{C}_{\mathsf{k}}(G)$. Then we have*

$$\rho(f) = \frac{|G|}{\dim(V)} \langle f, \chi_V^* \rangle id_V$$

Proof. Since $\mathcal{C}_{\mathsf{k}}(G) = Z(\mathsf{k}[G])$ the endomorphism $\rho(f)$ commutes with the action of G, and hence by Schur's lemma $\rho(f)$ is $\lambda.\mathrm{id}_V$ for some $\lambda \in \mathsf{k}$. To calculate the scalar λ note that $\mathrm{tr}(\lambda.\mathrm{id}_V) = \lambda.\dim(V)$, hence we see that

$$\begin{aligned} \lambda &= \frac{1}{\dim(V)} \sum_{g \in G} f(g)\mathrm{tr}(\rho(g)) \\ &= \frac{|G|}{\dim(V)} \langle f, \chi_V^* \rangle. \end{aligned}$$

$\square$

Definition 4.10. For V be an irreducible representation let

$$c_V = \frac{\dim(V)}{|G|} \sum_{g \in G} \chi_V(g^{-1}) e_g \in \mathsf{k}[G].$$

Since χ_V is a class function, so is c_V, indeed $c_V = \frac{\dim(V)}{|G|} \chi_V^*$.

Notice that if V is the trivial representation, then c_V is just the element I_G we studied earlier. Moreover Lemma 4.9 and Theorem 4.5 immediately show the following:

Lemma 4.11. *Let (W, ρ) be a representation of G, and let $W = \bigoplus_{j \in J} W^j$ be its isotypical decomposition. Then $\rho(c_V)$ is the projection to the isotypical summand corresponding to V.*

Proof. It is enough to show that $\rho(c_V)$ restricts to the identity on any irreducible summand of W isomorphic to V, and to zero on any irreducible summand of W not isomorphic to V. But by Lemma 4.9 $\rho(c_V)$ acts on W by the scalar

$$\frac{\dim(V)}{\dim(W)}\langle \chi_V^*, \chi_W^* \rangle,$$

which by Theorem 4.5 is clearly 1 if $V \cong W$ and 0 otherwise. □

Let $\{U_j : j \in J\}$ be a complete set of representatives for the irreducible representations of G, and let $\chi_j = \chi_{U_j}$ and $c_j := c_{U_j} = \frac{\dim(U_j)}{|G|}\chi_j^*$. It follows from the above that given any representation (W, ρ) of G, we have

$$\sum_{j \in J} \rho(c_j) = 1, \quad \rho(c_j)^2 = \rho(c_j), \quad \rho(c_j)\rho(c_k) = 0 \text{ if } j \neq k.$$

Proposition 4.12. *The set $\{c_j : j \in J\}$ is a basis for the space of class functions $\mathcal{C}_{\mathsf{k}}(G)$. Thus the number of irreducible representations is equal to the number of conjugacy classes in G. Moreover the character $\{\chi_j : j \in J\}$ also form a basis for the space of class functions.*

Proof. Let $z \in \mathcal{C}_{\mathsf{k}}(G)$. Now z acts by the scalar $\lambda_j = \frac{|G|}{\dim(U_j)}\langle z, \chi_j^* \rangle$ on U_j. Thus it follows $\sum_{j \in J} \lambda_j c_j$ acts as z on any representation of G. Now considering the action of z on the unit e_e in the regular representation $\mathsf{k}[G]$ we see that

$$z = z \star e_e = \sum_{j \in J} \lambda_j c_j \star e_e = \sum_{j \in J} \lambda_j c_j.$$

Thus $\{c_j : j \in J\}$ spans the space $\mathcal{C}_{\mathsf{k}}(G)$. On the other hand, c_j is a nonzero multiple of χ_j^* for all $j \in J$, hence since the χ_j are linearly independent, the c_j must be also. Thus $\{c_j : j \in J\}$ is a basis for $\mathcal{C}_{\mathsf{k}}(G)$ (and hence $\{\chi_j : j \in J\}$ is also).

Since we have already seen that $\dim(\mathcal{C}_{\mathsf{k}}(G))$ is just the number of conjugacy classes in G, the proof is complete. □

Remark 4.13. When we work over $\mathbb{C}$ it is common to use, instead of $\langle -, - \rangle$, the Hermitian form

$$(f, g) = |G|^{-1} \sum_{k \in G} f(k)\overline{g(k)}$$

Since over the complex numbers $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ the above proofs show that over $\mathbb{C}$, the characters of irreducible representations form an orthonormal basis of the space $\mathcal{C}_{\mathbb{C}}(G)$.

We finish this section with a description of the regular representation. The character of the regular representation is easy to compute. Indeed using the basis $\{e_g : g \in G\}$ we see that $\mathrm{tr}(g, \mathsf{k}[G])$ is zero unless $g = e$ (since the matrix corresponding to g in this basis will consist of 1s and 0s with a 1 in the diagonal exactly when $gh = h$, that is when $g = e$). Thus

$$\chi_{\mathsf{k}[G]}(g) = \begin{cases} |G|, & \text{if } g = e, \\ 0, & \text{otherwise.} \end{cases}$$

It follows from this, and the fact that $\chi_V(e) = \dim(V)$ for every representation V, that

$$\dim(\mathrm{Hom}_G(\mathsf{k}[G], V)) = \langle \chi_{\mathsf{k}[G]}, \chi_V \rangle = \dim(V).$$

Now suppose that $V = U_j$. Then the dimension of this space is the number of times that U_j occurs in $\mathsf{k}[G]$, and so we see that

$$\mathsf{k}[G] \cong \bigoplus_{j \in J} U_j^{\oplus \dim(U_j)}.$$

as G-representations, and hence

$$|G| = \sum_{j \in J} \dim(U_j)^2 \tag{4.2}$$

Theorem 4.14 (Wedderburn). *Let $\{U_j : j \in J\}$ be a complete set of irreducible representations of G. Then there is a natural isomophism*

$$\theta \colon \mathsf{k}[G] \to \bigoplus_{j \in J} \mathit{End}_{\mathsf{k}}(U_j).$$

Proof. Since each U_j is a G-representation, there is a natural map

$$\theta_j \colon \mathsf{k}[G] \to \mathrm{End}_{\mathsf{k}}(U_j).$$

Let θ be the direct sum of these maps. Now since Equation 4.2 shows that the two algebras $\mathsf{k}[G]$ and $\bigoplus_{j \in J} \mathrm{End}_{\mathsf{k}}(U_j)$ have the same dimension, it is enough to show that θ is injective. But if $f \in \mathsf{k}[G]$ has $\theta(f) = 0$, then f acts as zero on any irreducible representation of G, and hence on any representation of G, and in particular is zero on the regular representation $\mathsf{k}[G]$. But then $f = f \star e_e = 0$, and we are done. $\square$

LINEAR REPRESENTATIONS: INDUCTION AND RESTRICTION OF REPRESENTATIONS

KEVIN MCGERTY

1. Representations and subgroups

In this section k *is an arbitrary field, unless otherwise stated.*

We now study the interaction between representations and subgroups. Suppose that G is a group and H is a subgroup. Given a representation (V, ρ) of G, we can "pull-back" the representation V to a representation of H, simply by restriction the homomorphism ρ to the subgroup H. (This is an example of the more general pull-back operation we discussed before, where if $\psi\colon K \to G$ is any group homomorphism, we can define a representation $\psi^*(V)$ of K via the composition $\rho \circ \psi$). The more subtle direction however is to see how starting with a representation of a subgroup H we can attach to it a representation of G.

We begin by describing a family of G-representations which are "controlled" by an H-invariant subspace: let (V, ρ) be a representation of G, and W a subspace of V invariant under H. Then for $g \in G$ the subspace $g(W)$ depends only on the H-coset of g and not g itself, since if $h \in H$ then

$$(gh)(W) = g(h(W)) = g(W).$$

Thus if $T = \{g_i : 1 \leq i \leq r\}$ is a set of representatives for the cosets of H in G, then

$$\sum_{g \in G} g(W) = \sum_{g_i \in T} g_i(W)$$

is clearly a subrepresentation of V – it is the subrepresentation *generated by* W – that is, it is the intersection of all G-subrepresentations of V containing W. As such this is the largest part of V we can hope to understand in terms of W, thus we suppose now that it is all of V. Moreover let us assume that the sum of the subspaces $g_i(W)$ is direct. Thus we suppose $V = \bigoplus_{1 \leq i \leq r} g_i(W)$. We claim that in this case the action of G on V is completely determined by the action of H on W and the above decomposition into the subspaces $g_i(W)$. Indeed if $g \in G$, the direct sum decomposition shows that it is enough to know how g acts on any vector in the subspaces $g_i(W)$. But gg_i lies in some H-coset, so we can find a $k \in \{1, 2, \ldots, r\}$ such that $gg_i = g_k h$ for some $h \in H$ and then

$$g(g_i(w)) = (gg_i)(w) = (g_k h)(w) = g_k(h(w)). \tag{1.1}$$

When V is a representation of G containing a W-invariant subspace W as above (so that V is the direct sum of the distinct G-translates of W) we say that V is the G-representation *induced* from W. We formalize this in a definition:

Date: March 2009.

Definition 1.1. Let (V, ρ) be a representation of G, and W an H-invariant subspace of V. We say that V is induced from W if from some (and hence any) choice of H-coset representatives $\{g_i : 1 \leq i \leq r\}$ we have $V = \bigoplus_i g_i(W)$.

Lemma 1.2. *Suppose that (V, ρ) is a G-representation and W is an H-invariant subspace. Then V is induced from W if and only if W generates V as a G-representation and $\dim(V) = \frac{|G|}{|H|}\dim(W)$. Moreover, any two representations V_1, V_2 which are induced from subspaces which are isomorphic as H-representations are themselves isomorphic.*

Proof. Clearly the conditions are necessary for V to be induced from W, but they are also sufficient: if W generates V and $T = \{g_1, \ldots, g_r\}$ are H-coset representatives, we have $V = \sum_{i=1}^{r} g_i(W)$, so that this sum is direct if and only if

$$\dim(V) = \sum_{i=1}^{r} \dim(g_i(W)) = r.\dim(W).$$

Now if V_1 and V_2 are G-representations induced from subspaces W_1, W_2 where $W_1 \cong W_2$ as H-representations, Equation 1.1 shows that an isomorphism of H-representations between $\phi\colon W_1 \to W_2$ extends to isomorphism of G-representations between $\Phi\colon V_1 \to V_2$ via

$$\Phi(g_i(w)) = g_i(\phi(w)).$$

□

Example 1.3. Suppose that $G = S_3 = \langle s, t : s^2 = t^3 = 1, sts^{-1} = t^{-1}\rangle$ (so that we can take $s = (12)$ and $t = (123)$ say). Then let $H = \langle t \rangle$ be the cyclic group of order 3 in G. Assume that $\mathsf{char}(\mathsf{k}) \neq 3$, so that H has two nontrivial irreducible representations, given by $t \mapsto \omega^{\pm 1}$ where ω, ω^{-1} are the two nontrivial cube roots of 1 in k (so over $\mathbb{C}$ these are $e^{2\pi i/3}$ and $e^{4\pi i/3}$ respectively). If we let V be the two-dimensional representation of G

$$V = \{(a, b, c) \in \mathsf{k}^3 : a + b + c = 0\},$$

where G acts by permuting the coordinates, then the line L spanned by $(1, \omega, \omega^2)$ is an H-invariant subspace of V, and its s-translate $s(L)$ is distinct from it, so their direct sum is V. Thus V is induced from the H-representation L[1].

This gives an intrinsic description of what it means to say a representation of G is induced from a representation of H, but we also want a description of how we can construct a G-representation from an H-representation. One approach to this is to essentially to "reverse engineer" the previous construction, *i.e.* check that the above calculations can be used to construct a G-action, but we prefer a slightly more hands-free approach.

Suppose that H is a subgroup of G and V is the permutation representation of G coming from the G-set G/H. Thus $V = \mathsf{k}[X]$ is the vector space of functions on $X = G/H$. If $x = eH$ is the point of X corresponding to H itself, then the span of its indicator function e_H is a copy of the trivial representation of H, and clearly it generates V. Since the dimension of $\mathsf{k}[X]$ is $|G|/|H|$ it follows that $\mathsf{k}[X]$ is an

[1] If you're interested, notice that in characteristic 3 the representation V is *not* induced from a representation of H: the only H-invariant line is then the line spanned by $(1, 1, 1)$, which is also G-invariant.

induced representation. Now a function on G/H can be thought of as a function on G which is constant on the H-cosets[2]. Thus we have

$$\mathsf{k}[G/H] \cong \{f \colon G \to \mathsf{k} : f(gh) = f(g), \forall h \in H\}.$$

We define induction on H-representations in exactly the same fashion, simply replacing the trivial representation k of H with an arbitrary representation W.

Definition 1.4. Let (W, ψ) be a representation of H. We define the G-representation

$$\mathrm{Ind}_H^G(W) = \{f \colon G \to W : f(gh) = \psi(h)^{-1} f(g)\}$$

where G acts on $\mathrm{Ind}_H^G(W)$ by $g(f)(x) = f(g^{-1}x)$.

There is a natural map $\mathrm{ev} \colon \mathrm{Ind}_H^G(W) \to W$ given by $f \mapsto f(e)$. This map is of course not a map of G-representations (as W isn't a G-representation) but it is a map of H-representations, since

$$\mathrm{ev}(h(f)) = h(f)(e) = f(h^{-1}.e) = f(e.h^{-1}) = \psi(h^{-1})^{-1} f(e) = \psi(h)(\mathrm{ev}(f)).$$

(this is the reason for the inverse in the definition of induction). We now give a more explicit description of $\mathrm{Ind}_H^G(W)$. Let $T = \{g_i : 1 \leq i \leq r\}$ be a set of coset representatives for H (and assume that $g_1 = e$ is the representative for the subgroup H itself). Then for each i set

$$W^i = \{f \in \mathrm{Ind}_H^G(W) : f(g) \neq 0 \text{ only if } g \in g_i H\},$$

so that W^i depends only on the coset of H, not the choice of representative. Now clearly

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

The following lemma describes $\mathrm{Ind}_H^G(W)$ in terms of this decomposition.

Lemma 1.5. *Suppose that W is an H-representation. If $T = \{g_i : 1 \leq i \leq r\}$ is a set of representative for the H-cosets in G with $g_1 = e$, then the map*

$$\psi_i \colon W^i \to W,$$

given by $\psi_i(f) = f(g_i) = ev(g_i^{-1}(f))$ is an isomorphism of vector spaces, and ψ_1 is H-equivariant. Moreover the action of $g \in G$ on W^i is given in terms of the maps ψ_i by:

$$g(\psi_i^{-1}(w)) = \psi_k^{-1}(h(w)), w \in W.$$

where $gg_i = g_k h$, for some (unique) $h \in H$.

Proof. Suppose that $f \in W^i$, and we have $g = g_i h \in g_i H$. By definition we have

$$f(g) = f(g_i h) = h^{-1} f(g_i),$$

so that f is determined by its value at g_i. Moreover, given an arbitrary vector $w \in W$ we can use the above equation to define a function $f \colon G \to W$ by

$$f(g) = \begin{cases} h^{-1}(w), & \text{if } g = g_i h, \text{ for some } h \in H, \\ 0, & \text{otherwise.} \end{cases}$$

which evidently lies in W^i. It follows that ψ_i is an isomorphism as claimed. We have already checked that $\psi_1 = \mathrm{ev}$ is H-equivariant, so that W^1 is an H-invariant

[2]Formally, if $f \colon Y \to \mathsf{k}$ is a function on a set Y, and $\pi \colon X \to Y$ is a map, then we can define $\pi^*(f) \colon X \to \mathsf{k}$ by $\pi^*(f)(x) = f(\pi(x))$ – another example of pullback.

subspace. Moreover, clearly $\psi_i = \psi_1(g_i^{-1}(f))$ if $f \in W^i$ and[3] $W^i = g_i(W^1)$ it follows that W^1 generates $\text{Ind}_H^G(W)$ and $\dim(\text{Ind}_H^G(W)) = \dim(W).|G|/|H|$, so that $\text{Ind}_H^G(W)$ is a G-representation induced from the subspace W^1.

Finally, to see the formula for the action of $g \in G$ on $\text{Ind}_H^G(W)$, we simply note that if $f \in \text{Ind}_H^G(W)$, then

$$g(f)(g_k) = f(g^{-1}g_k) = f(g_ih^{-1}) = hf(g_i) = h\psi_i(f)$$

and hence $\psi_k(g(f)) = h(\psi_i(f))$, and so $g(\psi_i^{-1}(w)) = \psi_k^{-1}(h(w))$ as claimed. □

Note that the last part of the Lemma above gives a more explicit description of induction: if W is an H-representation, and we pick representatives for the H-cosets $\{g_1, g_2, \dots g_r\}$, then we can describe the induced G-representation as follows. Let V be the direct sum of r copies of W, say $W_1 \oplus W_2 \oplus \dots \oplus W_r$. For $w \in W$ and any i, $(1 \leq i \leq r)$ write $w_i = (0, \dots, w, \dots, 0) \in V$ for the vector whose i-th entry is w and whose other entries are zero. Then the action of G is given by

$$g(w_i) = (h(w))_k, \tag{1.2}$$

(extended linearly to all of V) where $h \in H$ and $k \in \{1, 2, \dots, r\}$ are given by $gg_i = g_kh$.

Remark 1.6. This explicit description can be used as the definition[4] but then one has to check that Equation 1.2 defines a homomorphism from G to V (this is not hard to do however). It is also not clear that the definition does not depend on the choice of coset representatives, so one must also check whether these choices matter (but you can see they do not using Lemma 1.2). By taking the definition in terms of functions on G, we get a representation $\text{Ind}_H^G(W)$ without making any choices, and then if we pick coset representatives, Lemma 1.5 shows how to identify $\text{Ind}_H^G(W)$ with the more explicit picture above using the maps ψ_i.

Example 1.7. Let $G = S_3$ and assume k is ordinary for G. If we induce the trivial representation of $H \cong \mathbb{Z}/3\mathbb{Z}$ to the group S_3, we get the permutation representation on the cosets of H in G. This is a two-dimensional representation on which H acts trivially, and t acts with two eigenspaces of dimension 1 with eigenvalues 1 and -1. Thus since $\text{char}(\mathsf{k}) \neq 2$ it is a reducible G-representation[5]. On the other hand, if we induce either nontrivial one-dimensional representation of H, we obtain the two-dimensional irreducible representation V of G: indeed V is the sum of two eigenspaces for t and these give the two irreducible H-representations, and V is induced from either.

Proposition 1.8. *Let G be a group and H a subgroup, and W_1, W_2 representations of H. Then we have:*

(1) $\mathit{Ind}_H^G(W_1 \oplus W_2) = \mathit{Ind}_H^G(W_1) \oplus \mathit{Ind}_H^G(W_2)$.

---

[3]I said this wrong in class: given $f \in W^i$ we have $f(g) \neq 0$ only when $g \in g_iH$ which means $g_i^{-1}(f)(g) = f(g_ig) \neq 0$ only if $g_ig \in g_iH$, that is $g \in H$. Thus $f \in W^i \iff g_i^{-1}f \in W^1$, that is $W^i = g_i(W^1)$.

[4]This is the "reverse engineering" approach referred to above.

[5]If the field is of characteristic 2, so that $1 = -1$, then the representation is indecomposable but not irreducible.

(2) *If $H < K < G$ are a chain of subgroups, and W is an H-representation, then there is a natural isomorphism of G-representations:*

$$\mathit{Ind}_K^G(\mathit{Ind}_H^K(W)) \cong \mathit{Ind}_H^G(W)$$

Proof. For the first part it is clear that

$$\{f : G \to W_1 \oplus W_2\} = \{f : G \to W_1\} \oplus \{f : G \to W_2\},$$

and if W_1, and W_2 are H-invariant, this clearly yields a direct sum decomposition of $\mathrm{Ind}_H^G(W)$.

For the second part, the issue is just to unravel what $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ actually is: if $f \in \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$, then f is a function on G taking values in the space of functions from K to W (which has to obey some conditions to do with H and K, which we will work out in a moment). This is the same as a function from $G \times K$ to W: given $g \in G, k \in K$ write

$$f(g,k) = f(g)(k) \in W.$$

The condition that $f \in \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ says that $f(gk) = k^{-1}f(g)$, and so

$$f(gk)(k_1) = (k^{-1}f(g))(k_1) = f(g)(kk_1),$$

which when thinking of f as a function $G \times K \to W$ says $f(gk, k_1) = f(g, kk_1)$. Finally, the requirement that $f(g) \in \mathrm{Ind}_H^K(W)$ says that

$$f(g,kh) = h^{-1}f(g,k), \quad g \in G, k \in K, h \in H.$$

Thus we have shown that the functions in $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ are

$$\{f : G \times K \to W : f(gk, k_1) = f(g, kk_1) \text{ and } f(g,kh) = h^{-1}f(g,k)\}.$$

But now we can see that this is just an over-elaborate way to describe $\mathrm{Ind}_H^G(W)$: indeed given such an f, we see that $f(g,k) = f(gk, e)$ so f is completely determined by its values on the subgroup $G \times \{e\} < G \times K$. Thus if we set $\tilde{f} : G \to W$ to be given by $g \mapsto f(g,e)$, the map $f \mapsto \tilde{f}$ gives an injection from $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W)$ to the space of functions from G to W. Moreover, the image clearly lies in $\mathrm{Ind}_H^G(W)$, since

$$\tilde{f}(gh) = f(gh,e) = f(g,h) = h^{-1}f(g,e) = h^{-1}\tilde{f}(g),$$

where the second equality holds because $h \in H < K$. Since the two spaces have dimension $\frac{|G|}{|H|}\dim(W)$ it follows the map $f \mapsto \tilde{f}$ is actually an isomorphism. Since it is easy to check that it respects the G action, we see that the two spaces are isomorphic as G-representations as required.

□

Remark 1.9. One can also give a slightly more abstract proof of the fact that the representations $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ and $\mathrm{Ind}_H^G(W)$ are isomorphic as follows[6]: By using the map $\psi_1^{-1} : W \mapsto W^1$ (where ψ_1 is the map in Lemma 1.5) we may indentify W with a subspace of $\mathrm{Ind}_H^G(W)$. Now the same Lemma shows that $\mathrm{Ind}_H^G(W)$ is induced from the subspace W, thus it is generated by W as a G-representation and has dimension $|G|/|H|\dim(W)$. On the other hand iterating the same argument we know that $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ is generated as a G-representation by the K-invariant subspace $\mathrm{Ind}_H^K(W)$ (thought of as a subspace of $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ in

[6]Which proof you prefer is up to you of course.

the same way W is identified with a subspace of $\mathrm{Ind}_H^G(W)$) and $\mathrm{Ind}_H^K(W)$ is generated by W as an H-representation. But then it is clear that the subspace $W < \mathrm{Ind}_H^K(W) < \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ generates $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ as a G-representation, and as $\mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ also has dimension $|G|/|H|\dim(W)$, thus Lemma 1.2 shows that $\mathrm{Ind}_H^G(W) \cong \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$ as required.

The fact that the action of G on an induced representation is completely determined the action of H on the subspace it is induced from is made precise by the following theorem.

Theorem 1.10. *(Frobenius reciprocity): Suppose that V is a G-representation and U is an H-representation. Then we have a natural isomorphism*

$$Hom_H(Res_H^G(V), U) \cong Hom_G(V, Ind_H^G(U))$$

Proof. Suppose that $\phi\colon V \to U$ is an H-equivariant linear map. Then define a map Φ from V to functions from G to U by sending $v \in V$ to the function $\Phi(v)$ given by

$$g \mapsto \phi(g^{-1}(v)), \quad \forall g \in G.$$

Let us check how the map $\phi \mapsto \Phi$ interacts with the action of G and H. We have for $g, k \in G$ and $h \in H$,

$$\begin{aligned} g(\Phi(v))(kh) = \Phi(v)(g^{-1}kh) &= \phi((g^{-1}kh)^{-1}v) \\ &= \phi(h^{-1}k^{-1}g(v)) \\ &= h^{-1}\phi(k^{-1}g(v)) \\ &= h^{-1}(\Phi(g(v))(k)). \end{aligned}$$

This shows both that $v \mapsto \Phi(v)$ is G-equivariant and that $\Phi(v) \in \mathrm{Ind}_H^G(U)$. Thus if we set I to be the map which sends ϕ to Φ we have shown I maps H-equivariant maps from V to U into G-equivariant linear maps from V to $\mathrm{Ind}_H^G(U)$.

On the other hand, recall the evaluation map $\mathrm{ev}\colon \mathrm{Ind}_H^G(U) \to U$ given by $\mathrm{ev}(f) = f(e)$. This is an H-equivariant map. If $\theta \in \mathrm{Hom}_G(V, \mathrm{Ind}_H^G(U))$ then clearly the composition $\mathrm{ev} \circ \theta$ is an H-equivariant linear map from V to U. Hence if we set $J(\theta) = \theta \circ \mathrm{ev}$ we get a map

$$J\colon \mathrm{Hom}_G(V, \mathrm{Ind}_H^G(U)) \to \mathrm{Hom}_H(\mathrm{Res}_H^G(V), U)$$

It is easy to see that $J(I(\phi)) = \phi$, and similarly you can show that $I(J(\theta)) = \theta$, so that I and J are isomorphism as claimed. □

Remark 1.11. If we assume that k is ordinary for G, then the spaces $\mathrm{Hom}_G(V, \mathrm{Ind}_H^G(U))$ determine $\mathrm{Ind}_H^G(U)$ up to isomorphism, since taking V to be irreducible, the dimension of this Hom-space is just the multiplicity of the irreducible representation V in $\mathrm{Ind}_H^G(U)$.

1.1. **Induction and characters.** *For the rest of this section we assume that* k *is ordinary for G.*

We may respell this result in terms of characters as follows: if V is a representation of G and U an representation of H, and we set χ to be the character of V, ψ the character of U and ψ_U^G the character of $\mathrm{Ind}_H^G(U)$. Then Frobenius reciprocity becomes the equation:

$$(\chi_{V|H}, \psi_U)_H = (\chi_V, \psi_U^G)_G.$$

(where $\chi_{|H}\colon H \to \mathsf{k}$ is the function χ restricted to H).

Since induction commutes with taking the direct sum of representations, the map $\psi \mapsto \psi^G$ extends to a linear map from $\mathcal{C}_\mathsf{k}(H)$ to $\mathcal{C}_\mathsf{k}(G)$ (which we will also write as $f \mapsto f^G$). Moroever, the restriction of characters also obviously extends to a map between the spaces of class function: if $p \in \mathcal{C}_\mathsf{k}(G)$ then $p_{|H}$ the restriction of p to H lies in $\mathcal{C}_\mathsf{k}(H)$ (since if a function has constant values on G-conjugacy classes, it certainly has constant values on H-conjugacy classes).

Since the form $(\cdot,\cdot)_G$ is nondegenerate on class function, the map on characters of H given by $\psi \mapsto \psi^G$ is completely determined by the restriction map from $\mathcal{C}_\mathsf{k}(G)$ to $\mathcal{C}_\mathsf{k}(H)$: indeed if $\{\chi_i : i \in \hat{G}\}$ are the irreducible characters of G, they form a basis for the space of class functions $\mathcal{C}_\mathsf{k}(G)$ and by orthogonality

$$\psi^G = \sum_{i \in \hat{G}} (\chi_i, \psi^G)_G \chi_i = \sum_{i \in \hat{G}} (\chi_{i|H}, \psi)_H \chi_i.$$

We use this to give an explicit expression for the character of an induced representation. Note that we want a map from class functions on H to class functions on G which is compatible with the bilinear forms on each as required by Frobenius reciprocity. Given any function $\psi \in \mathsf{k}[H]$ we can extend it to a function on G by setting its values outside H to be zero. Let $j\colon \mathsf{k}[H] \to \mathsf{k}[G]$ denote this map, so that

$$j(\psi)(g) = \begin{cases} \psi(g), & \text{if } g \in H, \\ 0, & \text{if } g \notin H. \end{cases}$$

Now if $f \in \mathcal{C}_\mathsf{k}(H)$ then $j(f)$ is not usually in $\mathcal{C}_\mathsf{k}(G)$. We fix this in the simplest way: averaging over G. Let $A^G\colon \mathsf{k}[G] \to \mathcal{C}_\mathsf{k}(G)$ be the projection

$$A^G(f)(x) = |G|^{-1} \sum_{g \in G} f(g^{-1}xg),$$

The composition of these maps $\psi \mapsto A^G(j(\psi))$ is a map from $\mathcal{C}_\mathsf{k}(H)$ to $\mathcal{C}_\mathsf{k}(G)$.

Lemma 1.12. *Let G and H be as above. Then*

(1) *For $f_1, f_2 \in \mathsf{k}[G]$ we have*

$$(A^G(f_1), f_2)_G = (f_1, A^G(f_2))_G.$$

(2) *For $p \in \mathcal{C}_\mathsf{k}(G)$ and $q \in \mathcal{C}_\mathsf{k}(H)$ we have*

$$(p_{|H}, q)_H = \frac{|G|}{|H|}(p, j(q))_G.$$

Proof. For the first part, we compute to see that:

$$\begin{aligned}
(A^G(f_1), f_2) &= |G|^{-1} \sum_{g \in G} A^G(f_1)(g) f_2(g^{-1}) \\
&= |G|^{-2} \sum_{g \in G} f_2(g^{-1}) \sum_{k \in G} f_1(k^{-1}gk) \\
&= |G|^{-2} \sum_{g,k \in G} f_1(k^{-1}gk) f_2(g^{-1}) \\
&= |G|^{-2} \sum_{g_1,k_1 \in G} f_1(g_1^{-1}) f_2(k_1^{-1}g_1k_1) \\
&= (f_1, A^G(f_2)).
\end{aligned}$$

where in the second last equality we set $g_1 = k^{-1}g^{-1}k$ and $k_1 = k^{-1}$.

For the second part, we have

$$\begin{aligned}(p, j(q))_G &= |G|^{-1} \sum_{g \in G} p(g)j(q)(g^{-1}) \\ &= |G|^{-1} \sum_{g \in G : g^{-1} \in H} p(g)q(g^{-1}) \\ &= |G|^{-1} \sum_{g \in H} p(q)q(g^{-1}) \\ &= \frac{|H|}{|G|}(p_{|H}, q)_H.\end{aligned}$$

□

This makes it easy to obtain a formula for the induced character.

Proposition 1.13. *Let $\psi \in \mathcal{C}_{\mathsf{k}}(H)$. Then we have*

$$\psi^G(g) = |H|^{-1} \sum_{x \in G : x^{-1}gx \in H} \psi(x^{-1}gx).$$

Proof. Let $A_H^G \colon \mathcal{C}_{\mathsf{k}}(H) \to \mathcal{C}_{\mathsf{k}}(G)$ be the map $\psi \mapsto \frac{|G|}{|H|}A^G(j(\psi))$. Then if $\chi \in \mathcal{C}_{\mathsf{k}}(G)$ we see

$$\begin{aligned}(\chi, A_H^G(\psi)) &= \frac{|G|}{|H|}(\chi, A^G(j(\psi)))_G \\ &= \frac{|G|}{|H|}(A^G(\chi), j(\psi)) \\ &= \frac{|G|}{|H|}(\chi, j(\psi))_G \\ &= (\chi_{|H}, \psi)_H,\end{aligned}$$

where in the second equality we use part (a) of Lemma 1.12, in the third equality the fact that χ is already a class function, so $A^G(\chi) = \chi$, and in the fourth equality we use part (b) of the same Lemma. But then $\psi \mapsto A_H^G(\psi)$ satisfies the character version of Frobenius reciprocity, and so as we saw above this uniquely characterizes the induction map on characters, so that $\psi^G = A_H^G(\psi)$. Since clearly

$$A_H^G(\psi)(x) = |H|^{-1} \sum_{g \in G : g^{-1}xg \in H} \psi(g^{-1}xg),$$

the result follows. □

We can also express the character of an induced representation in a form which is more useful when computing character tables. If $g \in G$, and $\mathcal{C}_G(g)$ is its conjugacy class in G, then $H \cap \mathcal{C}_G(g)$ is stable under conjugation by H, thus it is a union of H-conjugacy classes. Pick representatives $h_1, h_2, \ldots, h_s$ for the distinct H conjugacy classes, so that we have[7]

$$\mathcal{C}_G(g) \cap H = \bigsqcup_{i=1}^{s} \mathcal{C}_H(h_i).$$

[7]The symbol $\bigsqcup$ denotes a disjoint union.

where for $x \in H$, we write $\mathcal{C}_H(x)$ for the conjugacy class of x in H. We want to write, for $\psi \in \mathcal{C}_{\mathsf{k}}(H)$, the values of ψ^G in terms of the h_i.

Lemma 1.14. *Let $g \in G$ and $\psi \in \mathcal{C}_{\mathsf{k}}(H)$. If $h_1, h_2, \dots, h_s$ are representatives for the distinct H-conjugacy classes in $\mathcal{C}_G(g) \cap H$ then*

$$\psi^G(g) = \sum_{i=1}^{s} \frac{|Z_G(g)|}{|Z_H(h_i)|}\psi(h_i).$$

Proof. Let $X = \{x \in G : x^{-1}gx \in H\}$ and let

$$X_i = \{x \in X : x^{-1}gx \in \mathcal{C}_H(h_i)\}.$$

Thus the set X is the disjoint union of the sets X_i, $(1 \leq i \leq s)$. Now by Proposition 1.13 we know that

$$\psi^G(g) = |H|^{-1}\sum_{x \in X}\psi(x^{-1}gx),$$

and so using the decomposition of X we have just obtained, and the fact that ψ is constant on H-conjugacy classes we see

$$\begin{aligned}\psi^G(g) &= |H|^{-1}\sum_{i=1}^{s}\big(\sum_{x \in X_i}\psi(x^{-1}gx)\big)\\ &= |H|^{-1}\sum_{i=1}^{s}|X_i|\psi(h_i).\end{aligned}$$

Thus to complete the proof we need to calculate the numbers $|X_i|/|H|$. First we claim that X_i is acted on by the group $Z_G(g) \times H$ via $(y,h)(x) = yxh^{-1}$. Indeed if $x \in X_i$, then

$$(yxh^{-1})^{-1}g(yxh^{-1}) = h(x^{-1}(y^{-1}gy)x)h^{-1} = h(x^{-1}gx)h^{-1} \in \mathcal{C}_H(h_i),$$

since $x^{-1}gx$ is, and $h \in H$. Moreover, we claim that this action is transitive: indeed if $x_1, x_2 \in X_i$, then $x_2^{-1}gx_2 = hx_1^{-1}gx_1h^{-1}$ for some $h \in H$. But then

$$(x_1^{-1}h^{-1}x_2^{-1})g(x_2hx_1^{-1}) = g$$

so that $x_2hx_1^{-1} = y \in Z_G(g)$, and hence $x_2 = yx_1h^{-1}$ as required. But now to calculate the size of X_i, we may use the orbit-stabilizer theorem, and simply calculate the stabilizer of a point in X_i. Suppose that x_0 is such that $x_0^{-1}gx_0 = h_i$. Then the stabilizer of x_0 in $Z_G(g) \times H$ is

$$\{(y,h) \in Z_G(g) \times H : yx_0h^{-1} = x_0\}$$

which is just the set $\{(x_0hx_0^{-1}, h) \in G \times H : x_0hx_0^{-1} \in Z_G(g)\}$. But $x_0hx_0^{-1} \in Z_G(g)$ if and only if $h \in Z_G(x_0^{-1}gx_0) = Z_G(h_i)$, so the map $(y,h) \mapsto h$ gives an isomorphism from the stabilizer of x_0 in $Z_G(g) \times H$ to $Z_H(h_i)$. Hence the orbit-stabilizer theorem shows

$$|X_i| = |Z_G(g)|.|H|/|Z_H(h_i)|.$$

Finally, rearranging the terms, this shows that $|X_i|/|H| = |Z_G(g)|/|Z_H(h_i)|$ as required. $\square$

An alternative way to prove this result is to use Frobenius reciprocity directly: the exercises give more details.