Chapter 1

Representation theory

Let k be a field. A k-algebra is a ring R together with a homomorphism $k \to R$ that maps k to the center of R.

We shall always study rings in which $1 \neq 0$, so that the map $k \to R$ is non-zero and hence injective. Thus, we always think of k as a subring of R. Conversely, if R is a ring containing a copy of k in the center of R, then R is a k-algebra. If I is a two ideal in a k-algebra R, then R/I becomes a k-algebra too.

For example, all the quotient rings of a polynomial ring $k[x_1, \ldots, x_n]$ are k-algebras.

Multiplication gives k an action on R making R a k-vector space. Similarly, if M is an R-module, then restricting the R-action to k makes M a k-vector space. Then the map $\rho : R \to \operatorname{End}_{\mathbb{Z}} M$ defining the module structure factors through $R \to \operatorname{End}_k M$. In fact, giving an R-module is the same thing as giving a k-vector space V and a k-linear ring homomorphism $R \to \operatorname{End}_k V$.

1.1 Group algebras

We will use the letter G to denote a group and will write the group operation multiplicatively.

Definition 1.1 Let k be a field and G a (finite) group. The group algebra kG is the k-vector space with basis $\{v_g \mid g \in G\}$ indexed by G endowed with the multiplication

$$v_g v_h := v_{gh},$$

extended k-linearly. ◊

Thus a typical element of kG is $\sum_{G \in G} \lambda_g v_g$ where $\lambda_g \in k$, and the product in kG is

$$\Big(\sum_{g \in G} \lambda_g v_g\Big)\Big(\sum_{h \in G} \mu_h v_h\Big) = \sum_{g \in G}\Big(\sum_{xy=g} \lambda_x \mu_y\Big) g.$$

One should check that this does make kG into a ring with identity, the identity being the element v_e where e is the identity element in G.

The subset $\{v_g \mid g \in G\}$ of kG is closed under multiplication and, in fact, is a group isomorphic to G. We therefore think of G as a subset of kG, and reinforce this perspective by a tendency to write g rather than v_g. Doing this, the identity $e \in G$ becomes is written as 1 because it is the identity in the ring kG.

The ring kG is commutative if and only if G is abelian. When G is not abelian (the usual case) we must take care to distinguish between left and right ideals, and between left and right kG-modules.

We will (usually) work with left modules.

A left kG-module is also called a representation of G over the field k. In particular, $\mathbb{C}G$-modules are often called complex representations of G.

Because k is a subring of kG, a kG-module is also a k-module, i.e., a vector space over k.

If V is a kG-module, then the action of kG on V gives a ring homomorphism $kG \to \operatorname{End}_k V$ into the ring of linear operators on V. If $\dim_k V = n$, then $\operatorname{End}_k V \cong M_n(k)$. Hence, giving an n-dimensional representation of G over k is the same as giving a ring homomorphism $kG \to M_n(k)$. Restricting this map to G gives a group homomorphism $\rho : G \to \mathrm{GL}_n(k)$. Conversely, if one is given a group homomorphism $\rho : G \to \mathrm{GL}_n(k)$, there is a unique extension of ρ to a ring homomorphism $kG \to M_n(k)$.

This was the point of view when group representation theory was first developed in the period 1895–1900 by Molien, Frobenius, and Burnside: a representation is a group homomorphism $\rho : G \to \mathrm{GL}_n(k)$. That is, one tries to realize, or represent, G as a group of matrices.

In fact, the group algebra was introduced in 1854 by Cayley in the same paper in which he introduced the notion of an abstract group.

Theorem 1.2 (Molien) *Let k be a field in which $|G| \neq 0$. Let M be a kG-module and $N \subset M$ a kG-submodule. Then there is a kG-submodule $L \subset M$ such that $M = L \oplus N$.*

Proof. Let L be any subspace of M such that $M = N \oplus L$, and let $\pi : M \to N$ be the projection with $\ker \pi = L$. Define $\phi : M \to N$ by

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

If $m \in N$, then $g^{-1}m \in N$, so $\pi(g^{-1}m) = g^{-1}m$; hence $\phi(m) = m$. Thus ϕ is a projection of M onto N, and $M = N \oplus \ker \phi$.

However, ϕ is a kG-module homomorphism because if $h \in G$, then

$$\phi(hm) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hm) = \frac{1}{|G|} \sum_{x \in G} hx\pi(x^{-1}m) = h\phi(m).$$

It follows that $\ker \phi$ is a kG-submodule of M. □

A simple kG-module is also called an irreducible representation of G.

Corollary 1.3 *Let k be a field in which $|G| \neq 0$. Every finite dimensional representation of G is a direct sum of irreducible representations.*

Proof. Molien's Theorem says that kG is a semisimple ring (see Proposition ??.??. □

Corollary 1.4 *Let k be a field in which $|G| \neq 0$. Then there are division rings $D_1, \ldots, D_t$ and positive integers $n_1, \ldots, n_t$ such that*

$$kG \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_t}(D_t).$$

Proof. This is the Wedderburn theorem for semisimple rings. □

In the context of the previous corollary each D_i is obtained as $D_i = \mathrm{End}_{kG} S_i$ where $S_1, \ldots, S_t$ are the distinct simple kG-modules. The dimension over k of S_i is $n_i \dim_k D_i$.

Theorem 1.5 *kG is semisimple if and only if* $\mathrm{char}\, k$ *does not divide $|G|$.*

Proof. We must show that if $|G|$ is zero in k, then kG is not semisimple. It is enough to show that kG itself is not a semisimple left kG-module.

Let $\varepsilon : kG \to k$ be the linear map defined by $\varepsilon(g) = 1$. Then ε is a ring homomoprhism, so $\mathfrak{m} := \ker \varepsilon$ is a a two-sided ideal in kG, and $kG/\mathfrak{m}$ is a left kG-module of dimension one. Notice that $\mathfrak{m}$ is the linear span of $\{g-1 \mid g \in G\}$.

If kG were semisimple, $\mathfrak{m}$ would have a complement, say kw, a left ideal such that $kG = \mathfrak{m} \oplus kw$. There is a kG-module isomorphism $kw \cong kG/\mathfrak{m}$, so w would be annihilated by every $g - 1$. If we write $w = \sum_{x \in G} \lambda_x x$, then the condition $gw = w$ implies that all λ_xs are the same, i.e., $w = \lambda_1 \sum_{x \in G} x$. But this implies that $\varepsilon(w) = \lambda_1 |G| = 0$, so $w \in \mathfrak{m}$. From this contradiction we deduce that kG is not semisimple. □

Remark. Suppose that M and N are kG-modules and $f : M \to N$ a k-linear map. Then f is kG-module homomorphism if and only if $f(xm) = xf(m)$ for all $x \in kG$ and $m \in M$. However, every element of kG is a k-linear combination of the elements in G, so f is a kG-module homomorphism if and only if $f(gm) = gf(m)$ for all $g \in G$ and $m \in M$.

1.2 Examples

Molien's theorem shows that in "good characteristic" the representation theory of G is completely determined by knowledge of its irreducible representations. Hence, we wish to determine all simple kG-modules. If we fix G the answer depends on the field.

Certainly every 1-dimensional kG-module is simple, so we begin by looking for the 1-dimensional representations.

The trivial representation. The trivial representation of G is that corresponding to the map $G \to \mathrm{GL}_1(k) = (k\backslash\{0\}, \cdot)$, $g \mapsto 1$. Thus, the trivial representation is the kG-module k with every g acting on it as the identity.

The sign representation. Let S_n be the n^{th} symmetric group and let $\varphi : S_n \to \{\pm 1\} \subset \mathrm{GL}_1(k)$ be the map defined by

$$\varphi(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is an even permutation} \\ -1 & \text{if } \sigma \text{ is an odd permutation} \end{cases}$$

The associated 1-dimensional representation of S_n is called the sign representation.

If $\operatorname{char} k \neq 2$ the sign and trivial representations of S_n are not isomorphic. One way to see this is to notice that their annihilators are different (remember that isomorphic modules have the same annihilator). The trivial representation is annihilated by all $1 - g$, $g \in G$. These elements span an ideal of kG called the augmentation ideal. However, if $\operatorname{char} k \neq 2$, and $\sigma \in S_n$ is an odd permutation, then $1 - \sigma$ acts on the sign representation as multiplication by $2 \neq 0$, so does not annihilate the sign representation.

1-dimensional representations. Let G be any group. A 1-dimensional representation of G is the same thing as a group homomorphism $\varphi : G \to GL_1(k)$. Since $\mathrm{GL}_1(k)$ is abelian the kernel of such a homomorphism must contain all elements of the form $xyx^{-1}y^{-1}$. Such an element is called the commutator of x and y, and is denoted by $[x, y]$. The subgroup of G generated by all commutators is called the commutator subgroup of G. It is a normal subgroup because

$$a[x, y]a^{-1} = [a, [x, y]][x, y].$$

The quotient $G/[G, G]$ is abelian, and if A is any abelian group

$$\{\text{homomorphisms } G \to A\} = \{\text{homomorphisms } G/[G, G] \to A\}.$$

Hence

$$\{\text{1-dimensional repns of } G\} = \{\text{1-dimensional repns of } G/[G, G]\}.$$

So, we need to determine all 1-dimensional representations of a finite abelian group A. We can write $A = A_1 \times \cdots \times A_n$ as a product of cyclic abelian groups. There is a corresponding decomposition

$$kA \cong kA_1 \times \cdots \times kA_r \cong kA_1 \oplus \cdots \oplus kA_r$$

of the group algebra as a product (or direct sum) of group algebras of cyclic abelian groups. Lemma **??** shows that the representation theory of a finite abelian group $A = A_1 \times \ldots \times A_n$ is completely determined by that for each A_i. Thus we need to determine the representation theory of the cyclic groups.

Lemma 2.1 *There is a ring isomorphism $k\mathbb{Z}_n \cong k[x]/(x^n - 1)$.*

Proof. We have $\mathbb{Z}_n \cong \langle g \mid g^n = 1\rangle$, so $k\mathbb{Z}^n = k \oplus kg \oplus kg^2 \oplus \cdots \oplus kg^{n-1}$. Let $\psi : k[x] \to k\mathbb{Z}_n$ be the ring homomorphism determined by $\psi(x) = g$; of course, we also insist that ψ is k-linear. This map is surjective and its kernel is $(x^n - 1)$, hence the result. □

This isomorphism says that $k\mathbb{Z}_n$-modules are the same things as $k[x]$-modules that are annihilated by $(x^n - 1)$. The theory of $k[x]$-modules shows that every $k\mathbb{Z}_n$-module is isomorphic to a direct sum of modules of the form

$$\frac{k[x]}{(f^d)}$$

where f is a monic irreducible polynomial such that f^d divides $x^n - 1$.

At one extreme we have the case when $\operatorname{char} k = p$ and $n = p$. In this case,

$$k\mathbb{Z}_p \cong \frac{k[x]}{(x^p - 1)} = \frac{k[x]}{(x-1)^p} \cong \frac{k[x]}{(x^p)}. \tag{2-1}$$

The equality in (**??**) follows from the fact that in characteristic p,

$$(a+b)^p = a^p + b^p;$$

this holds because the binomial coefficients $\binom{p}{i}$ are divisible by p for $1 \le i \le p-1$. The final isomorphism in (**??**) is induced by the ring isomorphism $k[x] \to k[x]$, $x \mapsto x + 1$. The isomorphism $k\mathbb{Z}_p \to k[x]/(x^p)$ is given by $g \mapsto x + 1$.

We have proven the following result.

Proposition 2.2 *If* $\operatorname{char} k = p$*, then every* $k\mathbb{Z}_p$*-module is a direct sum of modules of the form*

$$\frac{k[x]}{(x^i)} = \frac{k\mathbb{Z}_p}{(g-1)^p}.$$

More generally, $k\mathbb{Z}_{p^n} \cong k[x]/(x^{p^n})$ if $\operatorname{char} k = p$.

At the other extreme, we have the following result.

Lemma 2.3 *Suppose that* k *has a primitive* n^{th} *root of unity, say* ω*. Fix a generator,* g *say, for* $\mathbb{Z}_n$*. Then* $k\mathbb{Z}_n$ *has* n *distinct simple modules up to isomorphism, namely*

$$V_i := k\mathbb{Z}_n/(g - \omega^i), \qquad 0 \le i \le n-1.$$

Proof. As remarked above, $k\mathbb{Z}_n \cong k[x]/(x^n - 1)$ where $g \leftrightarrow x$ under the isomorphism. The hypothesis implies that $x^n - 1$ factors into a product of n distinct irreducibles over k, namely

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

Let M be a $k[x]$-module that is annihilated by $x^n - 1$. By the structure theorem for modules over a p.i.d., M is isomorphic to a direct sum of modules of the form $k[x]/(f^r)$ where f is irreducible and f^r divides $x^n - 1$. Hence M is a direct sum of modules of the form $k[x]/(x - \omega^i)$. □

Lemma 2.4 *Let $\rho, \rho' : G \to \mathrm{GL}_1(k)$ be group homomorphisms, and let V and V' be the corresponding 1-dimensional representations of G. Then $V \cong V'$ if and only if $\rho = \rho'$.*

Proof. The module V is, by definition, the vector space k with the action given by $g.v = \rho(g)(v)$ for $g \in G$ and $v \in k$. Now V is isomorphic to V' if and only if there is a k-linear isomorphism $\phi : V \to V'$ such that $\phi(g.v) = g.\phi(v)$ for all $g \in G$ and $v \in V$. The k-linear isomorphisms from k to itself are of the form $\phi(v) = \lambda v$ for some $0 \neq \lambda \in k$. Thus $V \cong V'$ if and only if there is a non-zero $\lambda \in k$ such that $\lambda\rho(g)(v) = \rho'(g)(\lambda v)$ for all $g \in G$ and $v \in k$. But $\rho'(g)$ is a k-linear map, so this equality holds if and only if $\rho = \rho'$. □

The natural representation of S_n. Let V be the k-vector space with basis $e_1, \ldots, \epsilon_n$ and define

$$\sigma.e_i := e_{\sigma i},$$

for $\sigma \in S_n$ and extend the action of σ to a k-linear action on all of V. We call this the natural representation of S_n. It is an example of a *permutation representation* (see below).

Lemma 2.5 *Suppose that* $\mathrm{char}\, k$ *does not divide $n!$. Then the natural representation of S_n is the direct sum of the trivial representation and an $(n-1)$-dimensional irreducible representation.*

Proof. Notice that $\sigma.(e_1 + \cdots + e_n) = e_1 + \cdots + e_n$ for all $\sigma \in S_n$. Hence the line spanned by $e_1 + \cdots + e_n$ is an S_n-submodule of V and is isomorphic to the trivial representation.

The map $f : V \to k$ defined by $f(\alpha_1 e_1 + \cdots + \alpha_n e_n) = \alpha_1 + \cdots + \alpha_n$ is easily seen to be an S_n-module map to the trivial representation, so $U := \ker f$ is an S_n-submodule of V. A basis for U is given by the elements $e_i - e_{i+1}$, $1 \leq i \leq n-1$.

Let W be a non-zero kS_n-submodule of U, and choose $0 \neq u = (\alpha_1, \ldots, \alpha_n) \in W$. Certainly, u has at least two non-zero entries. If only two of the entries in u are non-zero, then W contains $e_i - e_j$ for some $i \neq j$; now we could act by S_n to get every $e_p - e_{p+1} \in W$; since these elements span U, we have $W = U$.

Now suppose u has at least three non-zero entries. The non-zero entries in u can not all be the same because $f(u) = 0$ and $n! \neq 0$ in k. Permuting entries, we may therefore assume that $\alpha_1\alpha_2 \neq 0$ and $\alpha_1 \neq \alpha_2$. Now W contains

$$(\alpha_1 - \alpha_2)^{-1}\Big(\alpha_2 - \alpha_1(12)\Big).u = (0, \alpha_1 + \alpha_2, \alpha_3, \ldots, \alpha_n).$$

By induction, we may assume the lemma is true for S_{n-1}, so if G is the subgroup of S_n fixing 1,

$$kG.(0, \alpha_1 + \alpha_2, \alpha_3, \ldots, \alpha_n) = (0, *, *, \ldots, *) \cap \ker f \subset W.$$

This subspace of W has dimension $n-2$, and does not contain u, so $\dim W \geq n-1$, whence $W = U$. Thus U is simple. □

Permutation representations. Suppose G acts on a set X, i.e., we have a group homomorphism

$$\varphi : G \to S(X) := \{\text{bijective maps } X \to X\}.$$

We also write $gx := \varphi(x)$. Thus, the action of G on X is the same thing as a map $G \times X \to X$, $(g, x) \mapsto gx$, such that $g.(h.x) = (gh).x$ for all $g, h \in G$ and $x \in X$.

Now fix a field k and let V denote the k-vector space with basis $\{e_x \mid x \in X\}$. We make V into a representation of G by defining $g.e_x := e_{gx}$ for all $g \in G$ and $x \in X$, and extending this action linearly. Check that this makes V a kG-module.

We call V a permutation representation of G.

If $O = Gx$ is an orbit in X, then

$$V_O := \bigoplus_{gx \in O} ke_{gx}$$

is a subrepresentation. Further, since V is a disjoint union of orbits there is an analogous decomposition of V as a direct sum of submodules, $V = \oplus_{\text{orbits } O} V_O$.

Example 2.6 Suppose that $\operatorname{char} k \neq 2$. Let $G = S_3$, the symmetric group. What is the endomorphism ring of the 2-dimensional irreducible representation V? Suppose that $\phi : V \to V$ is a kS_3-module homomorphism. Then ϕ commutes with the action of S_3. Remember that $V \subset ke_1 + ke_2 + ke_3$ is the kernel of the linear form defined by $\lambda(e_i) = 1$ for all i.

Now (12) has two distinct eigenvectors $e_1 - e_2$ and $e_1 + e_2 - 2e_3$ with eigenvalues -1 and 1, respectively. Hence ϕ must preserve each of these eigenspaces. Similarly, (13) has eigenvalues ± 1 and ϕ preserves those two eigenspaces. It follows that ϕ is multiplication by a constant. Hence $\operatorname{End}_{kS_3} V = k$. ◊

Since G is finite, kG is a finite dimensional vector spaces. Thus kG is left and right noetherian.

Proposition 2.7 *If G is a finite group kG has only a finite number of simple modules up to isomorphism.*

Proof. This is Corollary **??.??**. □

As already mentioned, a basic task of representation theory is to find all the representations of all finite groups over all fields. In particular, one must find the simple modules. The proposition shows this is a finite task. If $(\operatorname{char} k, |G| = 1)$, this finishes the task because all modules are direct sums of simple ones.

A module is indecomposable if it is not a direct sum of two non-zero modules. It is easy to see that every module is a direct sum of indecomposable ones. It is not so easy to see that over kG (or, more generally, over any finite dimensional k-algebra) every module is a direct sum of indecomposable ones *in a unique way*. Thus, to find all modules one must find all the indecomposable ones. For

example, we have already seen that over a field of characteristic p, $\mathbb{Z}_p$ has exactly $p+1$ indecomposable representations.

The question of whether kG has only finitely many indecomposable representations must have arisen at an early stage of representation theory. The answer is "no". For example, if $\operatorname{char} k = p$, then $k(\mathbb{Z}_p \times \mathbb{Z}_p) \cong k[x,y]/(x^p, y^p)$. Set $R = k[x,y]/(x^2, xy, y^2)$. For each $(\alpha, \beta) \in k^2$ define $M_{\alpha,\beta} = R/I_{\alpha,\beta}$ where $I_{\alpha,\beta}$ is the ideal $k(\alpha x + \beta y)$. Thus $M_{\alpha,\beta}$ is a two-dimensional representation of $k(\mathbb{Z}_p \times \mathbb{Z}_p)$. It's only submodules are itself, zero, and $k\bar{x} + k\bar{y}$. It follows that $M_{\alpha,\beta}$ is indecomposable. The annihilator of $M_{\alpha,\beta}$ is $I_{\alpha,\beta}$; since $I_{\alpha,\beta} \neq I_{\gamma,\delta}$ if (α,β) are distinct points of $\mathbb{P}^1$, $M_{\alpha,\beta} \ncong M_{\gamma,\delta}$ if $(\alpha,\beta) \neq (\gamma,\delta)$. Thus, if k is an infinite field of characteristic p, then the modules $M_{\alpha,\beta}$ provide infinitely many non-isomorphic indecomposable representations of $\mathbb{Z}_p \times \mathbb{Z}_p$.

The G-structure on $\operatorname{Hom}_k(M,N)$. Let M and N be (left!) kG-modules. Then $\operatorname{Hom}_k(M,N)$ becomes a left kG-module via

$$(g.f)(m) = gf(g^{-1}m) \text{ for } g \in G,\ m \in M. \tag{2-2}$$

To verify this we must check that $(hg).f = h.(g.f)$. If $m \in M$, then

$$\Big(h.(g.f)\Big)(m) = g\Big(h.f\Big)(g^{-1}m) = gh.f(h^{-1}g^{-1}(m) = ((gh).f)(m).$$

A particular case is when N is the trivial representation. We write $M^* := \operatorname{Hom}_k(M, k_{triv})$.

Example 2.8 (The discrete Heisenberg group) Let $G \subset \mathrm{GL}_3(\mathbb{Z}_n)$ be the subgroup consisting of the upper triangular matrices with ones on the diagonal, i.e., the elements of G are

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \qquad a, b, c \in \mathbb{Z}_n.$$

This is the finite Heisenberg group of order n^3. It is generated by

$$\alpha := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

A computation shows that

$$\alpha^{-1}\beta^{-1}\alpha\beta = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and this element is central. In terms of generators and relations,

$$G = \langle \alpha, \beta, z \mid \alpha^n = \beta^n = z^n = 1,\ \alpha^{-1}\beta^{-1}\alpha\beta = z,\ z\alpha = \alpha z,\ z\beta = \beta z \rangle.$$

The commutator subgroup of G is equal to its center $\langle z \rangle$. Since the commutator subgroup acts trivially on every 1-dimensional representation and $G/(z) \cong \mathbb{Z}_n \times \mathbb{Z}_n$, $\mathbb{C}G$ has n^2 1-dimensional modules up to isomorphism.

Now I describe an irreducible complex representation of dimension n. Let ω be a primitive n^{th} root of 1 and define a group homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ by

$$\rho(\alpha) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \qquad \rho(\beta) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \omega & 0 & \cdots & 0 & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 & 0 \\ \vdots & & & & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & \omega^{n-1} \end{pmatrix}$$

Notice that $\rho(\beta)\rho(\alpha) = \omega\rho(\alpha)\rho(\beta)$, so ρ really does extend to a group homomorphism $G \to \mathrm{GL}_n(\mathbb{C})$. To see that this action on $\mathbb{C}^n$ makes $\mathbb{C}^n$ an irreducible representation, let m be a non-zero element of $\mathbb{C}^n$. First, let's write $e_1, \ldots, e_n$ for the ordered basis of $\mathbb{C}^n$ with respect to which we wrote these matrices. Thus, $\alpha.e_i = e_{i+1}$ (where $e_{n+1} = e_n$) and $\beta.e_i = \omega^{i-1}e_i$. Write $m = \sum \lambda_i e_i$. If $\lambda_i \neq 0$, then $e_i \in \mathbb{C}[\beta].m$. Hence the $\mathbb{C}G$-submodule of $\mathbb{C}^n$ generated by m contains some e_i. Now $\mathbb{C}[\alpha].e_i = \mathbb{C}^n$, so $\mathbb{C}G.m = \mathbb{C}^n$. This shows that $\mathbb{C}^n$ is a simple $\mathbb{C}G$-module.

Notice that z acts on this representation as multiplication by ω^{-1}. ◊

Proposition 2.9 *Let p be a prime and G the Heisenberg group of order p^3. Then G has p^2 1-dimensional representations and $p-1$ distinct irreducible irreducible representations of dimension p.*

Proof. Let V be an irreducible representation of $\mathbb{C}G$. Then $(z-\lambda)V = 0$ for some $\lambda \in \mathbb{C}$ by Corollary 3.5. Since $z^p = 1$, $\lambda^p = 1$ too.

If $\lambda = 1$, then V is an irreducible representation of $G/(z) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. There are exactly p^2 such representations.

Now suppose that $\lambda \neq 1$. Then λ is a primitive p^{th} root of 1. We just saw in the previous example that G has an irreducible representation of dimension p that is annihilated by $(z-\lambda)$. As λ varies over the distinct primitive p^{th} roots of unity we obtain $p-1$ different irreducible representations of dimension p. These, together with the 1-dimensional representations give a complete list of the irreducible representations because $(p-1)p^2 + (p^2).1 = p^3 = |G|$. □

1.3 Basic results

Of course we identify the field k with the subring $k.1$ of kG. Of course, k is in the center of kG.

Lemma 3.1 *Let R be any ring, $Z(R)$ its center, and M a left R-module. There is a ring homomorphism $\Phi : Z(R) \to \mathrm{End}_R M$, defined by $\Phi(z) = \phi_z$ where*

$\phi_z : M \to M$ is given by $\phi_z(m) = zm$. Moreover, the image of Φ is contained in the center of $\mathrm{End}_R M$.

Proof. First, if $r \in R$, then $\phi_z(rm) = zrm = rzm = r\phi_z(m)$, so $\phi_z \in \mathrm{End}_R M$. If $\psi \in \mathrm{End}_R M$, then $\phi_z\psi(m) = z\psi(m) = \psi(zm) = \psi\phi_z(m)$ so $\phi_z\psi = \psi\phi_z$; i.e., the image of Φ is contained in the center of $\mathrm{End}_R M$.

It remains to show that Φ is a ring homomorphism. This is easy. □

Hence if M is a simple kG-module, the map from $Z(kG)$ to the division ring $D = \mathrm{End}_{kG} M$ sends k to the center of D. Since kG has finite dimension over k so do M and D.

Lemma 3.2 *Let R be a commutative domain. If R contains a field k and* $\dim_k R < \infty$, *then R is a field.*

Proof. Let $0 \neq x \in R$ and define $\alpha : R \to R$ by $\alpha(r) = xr$. Because R is a domain, α is iunjective, and hence surjective because $\dim_k R < \infty$. Hence $1 = \alpha(r)$ for some r, and we deduce that r is the inverse of x. Thus R is a field. □

Lemma 3.3 *Let k be an algebraically closed field and D a division ring that contains a copy of k in its center. If* $\dim_k D < \infty$, *then $D = k$.*

Proof. Let x be any non-zero element of D. The subring $R = kx + kx^2 + \ldots$ of D is a domain and is commutative. It is also finite dimensional because D is, so it is a field by Lemma 3.2 But k is algebraically closed so $R = k$. Thus $x \in k$. □

Proposition 3.4 *If k is an algebraically closed field and V an irreducible kG-module, then* $\mathrm{End}_{kG} V = k$.

Corollary 3.5 *Let k be an algebraically closed field, V an irreducible kG-module, and $z \in Z(G)$ a central element of G. Then $(z - \lambda)V = 0$ for some $\lambda \in k$.*

Proof. Recall that the action of $Z(kG)$ on V gives a ring homomorpphism $\phi : Z(kG) \to \mathrm{End}_{kG} V$. But that endomorphism ring is k, so $\phi(z) = \lambda$ for some $\lambda \in k$. In other words, if $v \in V$ then $zv = \lambda v$, whence $(z - \lambda)v = 0$. □

This corollary can sometimes be used to recognize when two irreducible representations are not isomorphic. Since isomorphic modules have the same annihilator, if $z \in Z(G)$ acts on V as multiplication by λ and on W as multiplication by $\mu \neq \lambda$, then $V \ncong W$. We use this argument in Example 2.8.

Theorem 3.6 *Suppose k is an algebraically closed field such that* $\mathrm{char}\, k$ *does not divide $|G|$. Then*

$$kG \cong M_{n_1}(k) \oplus \cdots \oplus M_{n_t}(k)$$

where there are t different simple kG-modules, say $S_1, \ldots, S_t$, of dimensions $n_1, \ldots, n_t$.

Notice in particular, that $|G|$ is equal to the sum of the squares of the dimensions of the irreducible $\mathbb{C}G$-modules.

Proposition 3.7 *Suppose k is an algebraically closed field such that* char k *does not divide $|G|$. Then the number of irreducible representations of G is equal to the number of conjugacy classes in G.*

Proof. Because kG is semisimple, we have a Wedderburn decomposition

$$kG \cong M_{n_1}(k) \oplus \cdots \oplus M_{n_t}(k)$$

where t is the number of simple modules. From the Wedderburn decomposition we see that the center Z of kG has dimension t: it has basis given by the idempotents $e_1, \ldots, e_t$ where e_i is the identity element in $M_{n_i}(k)$.

If $\{g_1, \ldots, g_r\}$ is a conjugacy class in G, then $g_1 + \ldots + g_r$ is in Z. We call this a class sum.

Claim: The class sums form a basis for the center of kG. Proof: Certainly the different class sums are linearly independent. On the other hand, if $z = \sum_{g \in G} \lambda_g g$ is in the center of kG, then for every $x \in G$,

$$z = xzx^{-1} = \sum_{g \in G} \lambda_g xgx^{-1}.$$

Hence $\lambda_g = \lambda_{xgx^{-1}}$. In other words if $\{g_1, \ldots, g_r\}$ is a conjugacy class in G, then $\lambda_{g_i} = \lambda_{g_j}$ for all i, j. Hence $\lambda_{g_1} g_1 + \ldots + \lambda_{g_r} g_r = \lambda_{g_1}(g_1 + \ldots + g_r)$, so z is a linear combination of class sums. □

As the next example illustrates, it is sometimes possible to determine the dimensions of the irreducible representations rather easily by using the results in this section.

Example 3.8 (Dihedral Groups) The dihedral group of order $2n$ is

$$D_n := \{\sigma, \tau \mid \sigma^2 = \tau^n = 1,\ \sigma\tau\sigma = \tau^{-1}\}.$$

Suppose that char $k | \not| n$ so every representation of D_n over k is semisimple.

(1) Suppose that $n = 2m$ is even. There are two conjugacy classes with m elements, namely

$$\{\sigma, \sigma\tau^2, \sigma\tau^4, \ldots, \sigma\tau^{2m-2}\} \text{ and } \{\sigma\tau, \sigma\tau^3, \sigma\tau^5, \ldots, \sigma\tau^{2m-1}\}.$$

The center of D_{2m} is $\{1, \tau^m\}$. There are $m - 1$ conjugacy classes with two elements, namely

$$\{\tau, \tau^{-1}\},\ \{\tau^2, \tau^{-2}\},\ \ldots,\ \{\tau^{m-1}, \tau^{1-m}\}.$$

This is a total of $m+3$ conjugacy classes.

The commutator subgroup is generated by $\tau^2 = \sigma\tau^{-1}\sigma\tau$, so

$$\bar{G} := G/[G,G] \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Then $\bar{G}$, and hence G, has four distinct 1-dimensional representations, and all other irreducible representations have dimension ≥ 2. But $4.1^2 + (m-1).2^2 = 4m = |D_{2m}|$, so we conclude that D_{2m} has four 1-dimensional representations and $m-1$ two-dimensional irreducible representations.

(2) Now suppose that $n = 2m+1$ is odd. There is one conjugacy class with n elements, namely

$$\{\sigma, \sigma\tau^2, \sigma\tau^4, \ldots, \sigma\tau^{2m} = \sigma\tau^{n-1}, \sigma\tau^{2m+2} = \sigma\tau, \sigma\tau^3, \ldots, \sigma\tau^{2m-1} = \sigma\tau^{n-2}\}.$$

The center of D_{2m+1} is trivial. There are m conjugacy classes with two elements, namely

$$\{\tau, \tau^{-1}\},\ \{\tau^2, \tau^{-2}\},\ \ldots,\ \{\tau^m, \tau^{-m}\}.$$

This is a total of $m+2$ conjugacy classes.

The commutator subgroup is generated by $\tau^2 = \sigma\tau^{-1}\sigma\tau$, so equals $\langle\tau\rangle$, and

$$\bar{G} := G/[G,G] \cong \mathbb{Z}_2.$$

Then $\bar{G}$, and hence G, has two distinct 1-dimensional representations, and all other irreducible representations have dimension ≥ 2. But $2.1^2 + (m).2^2 = 4m + 2 = |D_{2m+1}|$, so we conclude that D_{2m+1} has two 1-dimensional representations and m two-dimensional irreducible representations. $\Diamond$

Example 3.9 (The quaternion group) Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the subgroup of the quaternion algebra $\mathbb{H}$. Although $Q \ncong D_4$, the representation theory of these two groups is in some naive sense the "same". (We will explain later why it is not really the same—compare the character tables.)

The center of Q is $\{\pm 1\}$ so there are two conjugacy classes of size one. There are three other conjugacy classes, namely $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$. Since there are five conjugacy classes, over $\mathbb{C}$, Q has four one-dimensional and one two-dimensional irreducible representation. This is the same as for D_4. $\Diamond$

Consider the irreducible representations of S_n. The conjugacy classes in S_n are in bijection with the partitions of n.

Representations of S_4. The partitions of 4 are

$$(1^4),\ (1^2, 2),\ (1, 3),\ (2, 2),\ 4.$$

We already know there are two 1-dimensional irreducibles. The only way to write 24 as a sum of five squares, one of which is 1, is

$$24 = 1^2 + 1^2 + 2^2 + 3^2 + 3^2.$$

We know this *without even trying to find the representations.*

Representations of S_5. The partitions of 5 are

$$(1^5),\ (1^3,2),\ (1,2^2),\ (1^2,3),\ (1,4),\ (2,3),(5),$$

so S_5 has 7 irreducible representations. We already know there are two 1-dimensional irreducible representations, and an irreducible representation of dimension 4, so that leaves four to find of dimensions a,b,c,d where $a^2+b^2+c^2+d^2 = 120-1^2-1^2-4^2 = 102$.

1.4 Characters

Throughout this section G denotes a finite group and all the representations we consider will have finite dimension.

Definition 4.1 Let V be a finite dimensional k-vector space and $\rho : G \to \mathrm{GL}(V)$ a representation of G. The character of the representation, denoted χ_ρ or χ_V, is the function $G \to k$ given by

$$\chi_V(g) = \mathrm{Tr}\,\rho(g),$$

the trace of $\rho(g)$. We call $\dim_k V$ the degree of χ_V. If V is an irreducible representation we call χ_V an irreducible character. ◊

It is clear that isomorphic representations have the same character. Theorem 4.5 below shows the converse is also true—this is a remarkable fact.

A class function on G is a function $\psi : G \to k$ that is constant on conjugacy classes, i.e., $\psi(xgx^{-1}) = \psi(g)$ for all $g, x \in G$. We write $\mathrm{Cl}(G)$ for the space of class functions.

A character is a class function because conjugate matrices have the same trace, i.e., the trace of a linear map does not depend on the choice of basis.

The class functions $G \to k$ form a k-vector space in an obvious way, i.e., $(\psi+\phi)(g) := \psi(g)+\phi(g)$. We can also multiply two class functions, $(\psi\phi)(g) := \psi(g)\phi(g)$, and their product is a class function too. Hence the class functions form a ring.

Each class function $\psi : G \to k$ extends in a unique way to a linear map $\psi : kG \to k$. We make use of this observation and evaluate class functions at elements of kG.

Now suppose that the base field is $\mathbb{C}$. We speak of complex characters to indicate that we are working over $\mathbb{C}$.

Lemma 4.2 *Let χ be complex character of G of degree n. Then*

1. $\chi(1) = n$;
2. $\chi(g)$ *is a sum of roots of unity, hence an algebraic integer;*

3. $\overline{\chi(g)} = \chi(g^{-1})$;

4. *if* $g \neq 1$, *then* $\mathsf{Re}\chi(g) < n$.

Proof. (1) The trace of the identity in $M_n(\mathbb{C})$ is n.

(2) If $g \in G$, we can view $\mathbb{C}^n$ as a representation of the cyclic group $\langle g \rangle$, and as such it decomposes into a direct sum of 1-dimensional $\langle g \rangle$ submodules. Thus the matrix for g may be diagonalized, and the diagonal entries are the eigenvalues $\lambda_1, \ldots, \lambda_n$ for g. Since $g^m = 1$ for some $m \geq 1$, each λ_i is an m^{th} root of unity (λ_i^r is an eigenvalue for g^r).

(3) If λ is a root of unity, then $\lambda^{-1} = \overline{\lambda}$. To see this, suppose that $\lambda^m = 1$. Then $\lambda\overline{\lambda}$ is a positive real number whose m^{th} power is equal to 1, whence $\lambda\overline{\lambda} = 1$.

(4) The real part of $\chi(g)$ is the sum of the real parts of the λ_i. However, if $g \neq 1$ some $\lambda_i \neq 1$, so the real part of λ_i is < 1. □

If χ is a class function we define a new class function $\overline{\chi}$ by

$$\overline{\chi}(g) := \chi(g^{-1})$$

for all $g \in G$. We call this the dual of χ. The next result explains this terminology.

Proposition 4.3 *Let M and N be finite dimensaional kG-modules, and view $H = \mathrm{Hom}_k(M, N)$ as a kG-module via (2-2). Then*

$$\chi_H = \overline{\chi_M}\chi_N.$$

In particular, $\chi_{M^*} = \overline{\chi_M}$.

Proof. Choose bases $e_1, \ldots, e_m$ for M and $f_1, \ldots, f_n$ for N. Fix $g \in G$ and write

$$g^{-1}.e_j = \sum_{i=1}^{m} \alpha_{ij} e_i \qquad g.f_j = \sum_{i=1}^{n} \beta_{ij} f_i.$$

A basis for $\mathrm{Hom}_k(M, N)$ is given by the maps θ_{ij} defined by

$$\theta_{ij}(e_\ell) := f_i \delta_{j\ell}.$$

Then

$$\begin{aligned}
(g.\theta_{ij})(e_s) &= g.\theta_{ij}(g^{-1}.e_s) \\
&= g.\theta_{ij}\Big(\sum_{p=1}^{m} \alpha_{ps} e_p\Big) \\
&= g.\Big(\alpha_{js} f_i\Big) \\
&= \alpha_{js} \sum_{t=1}^{n} \beta_{ti} f_i.
\end{aligned}$$

Thus

$$g.\theta_{ij} = \sum_{t,s} \alpha_{js}\beta_{ti}\theta_{ts},$$

and the trace of g acting on $H = \mathrm{Hom}_k(M,N)$ is

$$\chi_H(g) = \sum_{i,j} \alpha_{jj}\beta_{ii} = \Big(\sum_{j=1}^{m} \alpha_{jj}\Big)\Big(\sum_{i=1}^{n} \beta_{ii}\Big) = \chi_M(g^{-1})\chi_N(g) = \overline{\chi}_M(g)\chi_N(g).$$

This completes the proof of the first statement, and the second is given by observing that the character of the trivial representation is identically one. □

Let G be a finite group with t distinct conjugacy classes. By Proposition 3.7, $\mathbb{C}G$ has t different simple modules up to isomorphism. Label these $S_1, \ldots, S_t$ and let $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_t}(\mathbb{C})$ be the corresponding Wedderburn decomposition. Thus $n_i = \dim_{\mathbb{C}} S_i$. Let e_i be the identity element in $M_{n_i}(\mathbb{C}) = \mathrm{End}_{\mathbb{C}G}\, S_i$. Then $\{e_1, \ldots, e_n\}$ is complete set of orthogonal idempotents, labelled so that $e_i S_j = 0$ if $i \neq j$ and e_i acts on S_i as the identity. We adopt the following notation:

simple modules	S_1	S_2	$\cdots\cdots$	S_t
their dimensions	n_1	n_2	$\cdots\cdots$	n_t
irreducible characters	χ_1	χ_2	$\cdots\cdots$	χ_t
central idempotents	e_1	e_2	$\cdots\cdots$	e_t

Theorem 4.4 *The irreducible characters form a basis for the class functions.*

Proof. With the above notation it is clear that

$$\chi_i(e_j) = n_i\delta_{ij}.$$

It follows at once that $\{\chi_1, \ldots, \chi_t\}$ is linearly independent. Since the number of conjugacy classes is t, $\dim_k \mathrm{Cl}(G) = t$ and the result follows. □

Theorem 4.5 *If V and W are $\mathbb{C}G$-modules, then $V \cong W$ if and only if $\chi_V = \chi_W$.*

Proof. Let $S_1, \ldots, S_t$ be the distinct simple $\mathbb{C}G$-modules and $\chi_1, \ldots, \chi_t$ the corresponding irreducible characters. If $V \cong S_1^{a_1} \oplus \cdots \oplus S_t^{a_t}$, then $\chi_V = a_1\chi_1 + \ldots + a_t\chi_t$. The result now follows from the linear independence of the irreducible characters. □

We write $\chi_{reg} = \chi_{\mathbb{C}G}$ and call it the regular character.

Lemma 4.6 *If $x \in G$, then* $\chi_{reg}(x) = \begin{cases} |G| & \text{if } x = 1, \\ 0 & \text{if } x \neq 1. \end{cases}$

Proof. Since $\dim \mathbb{C}G = |G|$, $\chi_{reg}(1) = |G|$. If $x \neq 1$, then the action of x on $\mathbb{C}G$ by left multiplication permutes the basis elements $\{g \in G\}$ leaving none fixed so, with respect to that basis, the matrix for x has zeroes on the diagonal. □

Lemma 4.7 *With the above notation,*

$$e_j = \frac{n_j}{|G|} \sum_{x \in G} \chi_j(x^{-1})x.$$

Proof. By the Wedderburn decomposition $\chi_{reg} = n_1\chi_1 + \cdots + n_t\chi_t$. If $g \in G$, then $g^{-1}e_j$ acts on S_j as g^{-1} does, and on S_i as zero if $i \neq j$. Hence

$$\chi_{reg}(g^{-1}e_j) = \sum_{i=1}^{t} n_i\chi_i(g^{-1}e_j) = n_j\chi_j(g^{-1}).$$

On the other hand, if we write $e_j = \sum_{x \in G} \lambda_x x$, the previous lemma shows that

$$\chi_{reg}(g^{-1}e_j) = \sum_{x \in G} \lambda_x \chi_{reg}(g^{-1}x) = |G|\lambda_g.$$

Thus $\lambda_g = |G|^{-1}n_j\chi_j(g^{-1})$, as required. □

Definition 4.8 The Hermitian inner product of two characters χ and ξ is

$$(\chi, \xi) := \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\xi(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\xi(g^{-1}).$$

The norm of a character is

$$||\chi|| = \sqrt{(\chi, \chi)}.$$

◊

We saw in Lemma 4.2 that $\chi(g^{-1}) = \overline{\chi(g)}$ so $\chi(g)\chi(g^{-1})$, and hence (χ, χ) is a non-negative real number so the norm of χ is a non-negative real number.

Lemma 4.9 *Let χ and ξ be complex characters. Then*

1. $(\xi, \chi) = \overline{(\chi, \xi)}$;
2. $(\chi_1 + \chi_2, \xi) = (\chi_1, \xi) + (\chi_2, \xi)$;
3. $(\lambda\chi, \xi) = \lambda(\chi, \xi)$ *and* $(\chi, \lambda\xi) = \overline{\lambda}(\chi, \xi)$ *for all* $\lambda \in \mathbb{C}$

Theorem 4.10 *The irreducible characters form an orthonormal basis for the space of class functions. That is,* $(\chi_i, \chi_j) = \delta_{ij}$.

Proof. We have already seen that $\chi_i(e_j) = n_j\delta_{ij}$. Thus, by Lemma 4.7,

$$n_j\delta_{ij} = \chi_i(e_j) = \frac{n_j}{|G|}\sum_{x\in G}\chi_j(x^{-1})\chi_i(x) = n_j(\chi_i,\chi_j).$$

The result follows. □

Fourier coefficients. If χ is any class function, we can write

$$\chi = \sum_{i=1}^{t}\alpha_i\chi_i = \sum_{i=1}^{t}(\chi,\chi_i)\chi_i.$$

We call $\alpha_i = (\chi,\chi_i)$ the i^{th} Fourier coefficient of χ.

Corollary 4.11 *A character has norm one if and only if it is irreducible.,*

Proof. We have just seen that $||\chi_j|| = 1$ for all j. On the other hand if $\chi = \lambda_1\chi_1 + \ldots + \lambda_n\chi_n$, then $(\chi,\chi) = \lambda_1^2 + \cdots + \lambda_n^2$. However, if $\chi = \chi_V$ for some representation V, each λ_i is a non-negative integer and, if V is not irreducible, this sum is ≥ 2, so $||\chi_V|| \geq \sqrt{2}$. □

The character table. One of the basic steps in understanding a group is to compute its character table. This is a square array of numbers with one row for each irreducible character and one column for each conjgacy class. The entry corresponding to row χ_i and conjugacy class C_j is $\chi_i(g)$ where $g \in C_j$.

Warning. Although the number of irreducible $\mathbb{C}G$-modules equals the number of conjugacy classes in G *there is no natural bijection between the conjugacy classes and the complex irreducible representations.*

This comment is a little vague because I do not say what I mean by "natural". However, let's look at a special case to see the problem. Let G be a cyclic group of order n. Then each element of G is a conjugacy class, so we are saying that there is no natural bijection between the elements of G and the irreducible representations. The irreducible representations are given by the group homomorphisms $\alpha : G \to \mathrm{GL}_1(\mathbb{C})$. The image of α must be contained in the group μ_n of n^{th} roots of unity. So we are saying there is no natural bijection between the elements of G and the homomorphisms $\alpha : G \to \mu_n$.

More to say!

Theorem 4.12 (Frobenius's Orthogonality Relations) *1. The weighted rows of the character table are orthogonal, i.e., for all* $1 \leq i,j \leq t$,

$$\sum_{k=1}^{t}|C_k|\chi_i(C_k)\overline{\chi}_j(C_k) = \delta_{ij}|G|. \tag{4-3}$$

2. The columns of the character table are orthogonal, i.e., for all $1 \leq i,j \leq t$,

$$\sum_{k=1}^{t}\chi_k(C_i)\overline{\chi}_k(C_j) = \delta_{ij}\frac{|G|}{|C_i|}. \tag{4-4}$$

Proof. (1) This is a restatement of the result that the irreducible characters form an orthonormal basis, namely

$$\begin{aligned}\delta_{ij} &= (\chi_i, \chi_j) \\ &= \frac{1}{|G|}\sum_{x\in G}\chi_i(x)\overline{\chi}_j(x) \\ &= \frac{1}{|G|}\sum_{k=1}^{t}|C_k|\chi_i(C_k)\overline{\chi}_j(C_k)\end{aligned}$$

(2) Let M be the $t \times t$ matrix with ij^{th} entry

$$M_{ij} := \sqrt{\frac{|C_j|}{|G|}}\chi_i(C_j)$$

and let M^* be its conjugate transpose. Then (1) says that $MM^* = I$, so $M^*M = I$ too, and writing out what this means for each entry gives (2). □

1.5 Tensor product of representations.

We observed earlier that a product of class functions is again a class function. It is reasonable to ask if the product $\chi_V\chi_W$ of two characters is again a character and, if so, what is the representation of which it is the character.

The answer is this:

$$\chi_V\chi_W = \chi_{V\otimes W},$$

where $V \otimes_k W$ is the tensor product of V and W.

In brief, $V \otimes W$ is a vector space spanned by elements that are denoted by $v \otimes w$ where $v \in V$ and $w \in W$, and the action of G on $V \otimes W$ is defined by

$$g.(v \otimes w) := (gv) \otimes (gw).$$

Although $V \otimes W$ is spanned by elements $v \otimes w$, there are lots of linear dependence relations between them. It turns out that

$$\dim(V \otimes W) = \dim V \times \dim W$$

and if $\{v_i \mid i \in I\}$ and $\{w_j \mid j \in J\}$ are bases for V and W, then

$$\{v_i \otimes w_j \mid i \in I, j \in J\}$$

is a basis for $V \otimes W$.

Definition 5.1 Let V and W be k-vector spaces. Their tensor product, denoted $V \otimes_k W$, is the vector space spanned by all symbols $\{v \otimes w \mid v \in V, w \in W\}$ subject to the relations:

1. $(v_1 \pm v_2) \otimes w = v_1 \otimes w \pm v_2 \otimes w$;
2. $v \otimes (w_1 \pm w_2) = v \otimes w_1 \pm v \otimes w_2$;
3. $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$;

$\Diamond$

Confessions and Misgivings. It seems that almost everyone finds the definition of tensor product unsettling at first. I have postponed giving the definition for this reason. There are several different ways to define tensor product and all seem to have their disadvantages (and advantages).

One definition I like is the most abstract one wherein one does not define $V \otimes W$ as a particular set with certain structure but one defines it in terms of its properties. (The idea that one might define an object by its properties is reminiscent of Matthew 7:15-18 "Ye shall know them by their deeds".) This is a new kind of definition. An example will show you what I mean.

The cartesian product of two sets M and N is usually defined as the set of ordered pairs (m, n) is $m \in M$ and $n \in N$. But we could also define it as the set MN having the property that there are "natural" isomorphisms

$$\mathrm{Map}(MN, D) \cong \mathrm{Map}(M, \mathrm{Map}(N, D))$$

for all sets D. Of course it appears that the first definition is preferable because it is concrete. An obvious problem with the second definition is that we do not even know if there is a set MN with the stated property. And there might be more than one such set. And what do we mean by "natural"? Given all this, it is probably not easy for you to believe that the second definition is in many ways better!

In this spirit, here is how one defines the tensor product of two modules.

Definition 5.2 Let M be a right R-module and N a left R-module. Then $M \otimes_R N$ is the unique abelian group (up to unique isomorphism) with the property that for every abelian group D there is an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, D) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N, D)). \tag{5-5}$$

$\Diamond$

For this definition to begin to make sense we need the right-hand side of the isomorphism to be defined and for this we need to make $\mathrm{Hom}_{\mathbb{Z}}(N, D)$ into a right R-module. We do this by defining

$$(\theta.r)(n) := \theta(rn)$$

for $n \in N$, $r \in R$, and $\theta : N \to D$ a group homomorphism. It is straightforward to check that this does indeed make $\mathrm{Hom}_{\mathbb{Z}}(N, D)$ into a right R-module.

Notice that the right-hand side of (5-5 gives a contravariant functor $F : \mathsf{Ab} \to \mathsf{Ab}$ from the category of abelian groups to itself, namely

$$M \mapsto \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N, D)).$$

Whenever we have such a functor we can ask whether there is an abelian group G such that $F(D) \cong \mathrm{Hom}_{\mathbb{Z}}(G, D)$ for all D.

Claim: If there is such a G then G is unique up to unique isomorphism.

We then show that there is such a G, namely the quotient of the free abelian group with basis the elements of the Cartesian product $M \times N$ modulo the subgroup generated by all elements of the form

$$\begin{aligned} (mr, n) - (m, rn) \qquad & m \in M,\ n \in N,\ r \in R \\ (m_1 + m_2, n) - (m_1, n) - (m_2, n) \qquad & m_1, m_2 \in M,\ n \in N, \\ (m, n_1 + n_2) - (m, n_1) - (m, n_2) \qquad & m \in M,\ n_1, n_2 \in N. \end{aligned}$$

One usually writes $m \otimes n$ for the image of (m, n) in the quotient group.

This is certainly explicit, but is difficult to work with. In practice what one works with is the defining property (5-5).

Proof: Suppose that G and G' are such. Then taking D to be G and G' we see that $F(G) \cong \mathrm{Hom}_{\mathbb{Z}}(G', G)$ and

1.6 Applications of characters

Lemma 6.1 *Let N be a normal subgroup of G, and $\pi : G \to G/N$ the natural map. If $\rho : G/N \to \mathrm{GL}(V)$ is a representation of G/N, then*

1. *$\rho\pi : G \to \mathrm{GL}(V)$ is a representation of G;*
2. *ρ is irreducible if and only if $\rho\pi$ is;*
3. *$\dim_{\mathbb{C}} V = \chi_V(1) = \chi_V(x)$ for all $x \in N$.*

Proof. □

Lemma 6.1 shows that each representation of G/N determines a representation of G in an obvious way; we call this process lifting a representation from G/N to G.

Proposition 6.2 *Let $\rho : G \to \mathrm{GL}(V)$ be a representation. Then*

1. *$\ker\rho = \{x \in G \mid \chi_V(x) = \chi_V(1)$;*
2. *ρ determines a representation $\overline{\rho}$ of $G/\ker\rho$ and ρ is the lift of $\overline{\rho}$.*

Proposition 6.3 *It is possible to determine the following informations from the character table of G:*

1. *the order of G;*

2. *the size of the conjugacy classes;*

3. *the order of the normal subgroups;*

4. *whether G is a simple group.*

Proof. (1) We have $|G| = \sum_{k=1}^{t} \chi_i(1)^2$.

(2) If C is a conjugacy class, then

$$|C| = \frac{|G|}{\sum_{k=1}^{t} \chi_i(C)\overline{\chi}_i(C)}.$$

(4) Claim: G is not simple $\iff$ there is a non-trivial irreducible character χ and $1 \neq x \in G$ such that $\chi(x) = \chi(1)$.

Proof: Let $N \neq G$ be a normal subgroup of G. Then $G/N \neq 1$ so G/N has a non-trivial irreducible representation, say $\rho : G/N \to \mathrm{GL}(V)$. Then V becomes a representation of G too and $\chi_V(x) = \chi(1)$ for all $x \in N$. □

Recall that $\omega \in \mathbb{C}$ is called an algebraic integer if ω is the zero of a monic polynomial with coefficients in $\mathbb{Z}$.

Lemma 6.4 *Let z_j be the sum of the elements in the conjugacy class C_j. Then z_j acts on the simple module S_i as multiplication by*

$$\omega_{ij} := \frac{1}{n_i}|C_j|\chi_i(C_j).$$

Proof. By Schur's Lemma, $\mathrm{End}_{\mathbb{C}G} S_i = \mathbb{C}$, and left multiplication by z_j is a $\mathbb{C}G$-module endomorphism of S_i so $\chi_i(z_j) = n_i\omega$ for some $\omega \in \mathbb{C}$. However, $\chi_i(z_j) = |C_j|\chi_i(C_j)$ because z_j is the sum of the elements in C_j. □

Let $\rho_i : G \to \mathrm{GL}_{n_i}(\mathbb{C})$ be the i^{th} irreducible representation. Then

$$\omega_{ij} = \rho_i(z_j).$$

Lemma 6.5 *The number*

$$\omega_{ij} := \frac{|C_j|}{n_i}\chi_i(C_j)$$

is an algebraic integer.

Proof. We consider the *integral group algebra*

$$\mathbb{Z}G := \bigoplus_{g \in G} \mathbb{Z}g \subset \mathbb{C}G.$$

The class sums, $z_C = \sum_{x \in C} x$, form a $\mathbb{Z}$-basis for the center of $\mathbb{Z}G$ as C runs through the conjugacy classes in G. For simplicity we label these class sums as $z_1, \ldots, z_t$. Since the center of $\mathbb{Z}G$ is a ring there are elements $\alpha_{ijk} \in \mathbb{Z}$ such that

$$z_i z_j = \sum_{k=1}^{t} \alpha_{ijk} z_k.$$

Applying ρ_ℓ to this equality gives

$$\omega_{\ell i}\omega_{\ell j} = \sum_{k=1}^{t} \alpha_{ijk}\omega_{\ell k}$$

or

$$\sum_{k=1}^{t} \Big(\alpha_{ijk} - \delta_{jk}\omega_{\ell i}\Big)\omega_{\ell k} = 0$$

for all i, j and ℓ. Let A be the $t \times t$ matrix with jk^{th} entry α_{ijk} and let X be the $t \times 1$ column matrix whose k^{th} entry is $\omega_{\ell k}$. Then

$$(A - I\omega_{i\ell})X = 0.$$

Since $\rho_\ell(e_\ell) \neq 0$, $X \neq 0$. Hence $\omega_{i\ell}$ is an eigenvalue for A and hence a zero of the characteristic polynomial of A. But all the entries of A are integers, so that characteristic polynomial is a monic polynomial in $\mathbb{Z}[x]$. Hence $\omega_{i\ell}$ is an algebraic integer. □

Proposition 6.6 *The dimension of every complex irreducible representation of G divides $|G|$.*

Proof. By (4-3) and Lemma 6.4,

$$|G| = \sum_{k=1}^{t} |C_k|\chi_i(C_k)\overline{\chi}_i(C_k) = \sum_{k=1}^{t} n_i\omega_{ik}\overline{\chi}_i(C_k).$$

By Lemma 4.2, $\overline{\chi}_i(C_k)$ is an algebraic integer. Since the algebraic integers form a ring, $|G|/n_i$ is an algebraic integer. But the only rational numbers that are algebraic integers are the integers themselves, so $|G|/n_i \in \mathbb{Z}$. □

Lemma 6.7 *Let C be a conjugacy class and $\chi = \chi_V$ an irreducible character. If $(|C|, \dim V) = 1$ and $x \in C$, then either $\chi(x) = 0$ or $|\chi(x)| = \dim V$.*

Proof. Recall that $\dim V = \chi(1)$. Let $a, b \in \mathbb{Z}$ be such that $a|C| + b\chi(1) = 1$. Since V is a direct sum of x-eigenspaces with eigenvalues roots of unity, the number

$$\lambda := \frac{\chi(x)}{\chi(1)} == a|C|\frac{\chi(x)}{\chi(1)} + b\chi(x)$$

is of the form $(\varepsilon_1 + \cdots + \varepsilon_n)/n$ for some roots of unity ε_j, where $n = \dim V$.

Certainly, $|\lambda| \leq 1$. Suppose that $\chi(x) \neq \dim V$. Then $|\lambda| < 1$. We need to show that $\lambda = 0$.

Write m for the order of x. Let G be the Galois group of the polynomial $x^m - 1$ over $\mathbb{Q}$, and write

$$\beta := \prod_{\sigma \in G} \sigma(\lambda).$$

Now $\sigma(\lambda) = (\sigma(\varepsilon_1) + \cdots + \sigma(\varepsilon_n))/n$, so $|\sigma(\lambda)| \leq 1$. Hence $|\beta| < 1$. However, $\beta = \sigma(\beta)$ for all $\sigma \in G$, so $\beta \in \mathbb{Q}$. But β is also an algebraic integer, so is in $\mathbb{Z}$. Hence $\beta = 0$. Thus $\lambda = 0$. □

Lemma 6.8 *Let ρ be an irreducible representation with character $\chi = \chi_V$. If $|\chi(x)| = \dim V$, then $\rho(x) = \varepsilon \,\mathrm{id}_V$ and $\chi(x) = \varepsilon \dim V$ for some root of unity ε.*

Proof. Write $n = \dim V$. We can pick a basis for V so that $\rho(V) = \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_n)$. Then

$$n = |\chi(x)| \leq |\varepsilon_1| + \cdots + |\varepsilon_n| = n.$$

This forces $\varepsilon_1 = \cdots = \varepsilon_n$, whence the result. □

Theorem 6.9 (Burnside) *Let p and q be primes. There is no simple group of order $p^a q^b$ for any $a, b \geq 1$.*

Proof. Let G be a group of order $p^a q^b$. We will assume that G is simple and obtain a contradiction.

Certainly G is not abelian. Furthermore, the center of G must be $\{1\}$.

Let Q be a q-Sylow subgroup and suppose there is $1 \neq g \in Z(Q)$. Let C be the conjugacy class in G containing g and let $H := \{h \in G \mid gh = hg\}$ be the centralizer of g. Since g is not in the center of G, $H \neq G$. Since $Q \subset H$, $|C| = [G : H] = p^c$ for some $c > 0$.

Let's label the representations so that ρ_1 is the trivial representation. Now

$$0 = \chi_{reg}(g) = \sum_{i=1}^{t} n_i \chi_i(g) = 1 + \sum_{k=2}^{t} n_k \chi_k(g).$$

Let p be a prime number. If p divides n_k for all $k \geq 2$, then $p^{-1} \in \mathbb{Z}\chi_2(g) + \cdots + \mathbb{Z}\chi_t(g)$, so would be an algebraic integer and hence in $\mathbb{Z}$. Hence $(p, n_k) = 1$ for some k.

Hence $(|C|, n_k) = 1$. But $\chi_k(g) = \varepsilon \,\mathrm{id}_V$. □