1 The group algebra as distributions

If you are reading this and are/were not a student in this class, you might want to know that in between Chapters III and IV of these notes, we covered parts of Chapters 0 and 1 of *Noncommutative Algebra* by Dennis and Farb. We are now in a position to prove all three of the theorems from Section III.2, but first we pause to better understand the nature of the group algebra, which contributes so crucially by linking representation theory to ring theory. In this section $F$ is an arbitrary field.

**Proposition 1.1.** Any representation of $G$ has a canonical $F[G]$-module structure and vice versa, and these constructions are inverse and compatible with morphisms.

*Proof.* Given a representation $V$ of $G$, define the $F[G]$-action by the formula

$$(\sum_{g \in G} a_g g) \cdot v := \sum_{g \in G} a_g (g \cdot v).$$

On the other hand, if $W$ is an $F[G]$-module, then the $G$-action is defined by

$$g \cdot w := (1g) \cdot w.$$  

The rest is clear.

This proposition tells us that $G$-representations and $F[G]$-modules are equivalent, and in particular submodules/subrepresentations, quotients, and anything else defined by a universal property are the same in both contexts.

Although Proposition 1.1 is pleasantly tautological, there is a slightly longer explanation which generalizes better. Let’s assume from now on that $G$ is finite. Consider the space of functions $G \to F$, which we have previously denoted by $\text{Fun}(G)$. It is tempting to identify $\text{Fun}(G)$ with $F[G]$, and indeed there is a canonical linear isomorphism, but it is better to identify $F[G]$ with the space of distributions

$$\text{Dist}(G) := \text{Fun}(G)^*.$$  

Elements $\lambda \in \text{Dist}(G)$ can be thought of as measures, so that intuitively

$$\lambda(f) = \int_G f d\lambda.$$  

From this point of view we should identify $\sum_{g \in G} a_g g$ with the distribution $\sum_{g \in G} a_g \delta_g$, where the delta distribution $\delta_g : \text{Fun}(G) \to F$ sends $f \mapsto f(g)$.

One reason to use distributions for the group algebra is that they have the correct variance: whereas functions “pull back,” distributions “push forward.” If $\varphi : X \to Y$ is a map of finite sets and $\lambda \in \text{Dist}(X)$, the formula $(\varphi_* \lambda)(f) = \lambda(f \circ \varphi)$ defines a linear map

$$\varphi_* : \text{Dist}(X) \to \text{Dist}(Y).$$
This is compatible with the group algebra construction, which sends a group homomorphism \( G \to H \) to a ring homomorphism \( F[G] \to F[H] \).

The convolution \( \lambda \ast \mu \) of two measures \( \lambda, \mu \in \text{Dist}(G) \) is inspired by the formula

\[
\int_G f d(\lambda \ast \mu) = \int_G \int_G f(xy) d\lambda(x) d\mu(y).
\]

Consider the map \( \text{Fun}(G) \otimes \text{Fun}(G) \to \text{Fun}(G \times G) \) which sends \( f \otimes g \to f \otimes g \), the latter being defined by

\[
(f \otimes g)(x, y) := f(x)g(y).
\]

It is easy to see that this map is injective, hence an isomorphism for dimension reasons. Since \( f \otimes g \) and \( f \otimes g \) correspond under this isomorphism, we discard the latter notation and refer to both as \( f \otimes g \).

Dualizing yields a canonical isomorphism

\[
\text{Dist}(G) \otimes \text{Dist}(G) \cong \text{Dist}(G \times G)
\]
characterized as follows. Given \( \lambda, \mu \in \text{Dist}(G) \), then for “separable” functions

\[
f_1 \otimes f_2 \in \text{Fun}(G \times G)
\]

we have

\[
(\lambda \otimes \mu)(f_1 \otimes f_2) = \lambda(f_1)\mu(f_2).
\]

As with functions, we have confused \( \lambda \otimes \mu \) with its image in \( \text{Fun}(G \times G) \), which might more properly be called \( \lambda \otimes \mu \). The separable functions span \( \text{Fun}(G \times G) \) so this formula uniquely characterizes \( \lambda \otimes \mu \).

Let \( m : G \times G \to G \) be the group operation.

**Definition 1.2.** Given \( \lambda, \mu \in \text{Dist}(G) \), define their convolution by \( \lambda \ast \mu := m_*(\lambda \otimes \mu) \in \text{Dist}(G) \).

It is not hard to check that convolution gives \( \text{Dist}(G) \) the structure of an associative \( F \)-algebra with the unity element \( \delta_e \).

**Proposition 1.3.** The map \( F[G] \to \text{Dist}(G) \) determined by \( g \mapsto \delta_g \) is an isomorphism of \( F \)-algebras, where \( \text{Dist}(G) \) is given the convolution product.

**Proof.** We have already pointed out that this map is a linear isomorphism, so it remains to show that it is a ring homomorphism. By distributivity it suffices to check on the generators \( g = 1g \in F[G] \):

\[
gh \mapsto \delta_{gh} = \delta_g \ast \delta_h,
\]

where the last equality is a simple calculation.

Now Propositions 1.1 and 1.3 together imply that a \( G \)-representation has a canonical \( \text{Dist}(G) \)-module structure and vice versa. Let us explain this equivalence explicitly. Given a representation \( V \) of \( G \), the action of \( \lambda \in \text{Dist}(G) \) should be consistent with the formula

\[
\lambda \cdot v = \int_G g \cdot v \ d\lambda.
\]

To make sense of this, note that any \( v \in V \) gives rise to a function \( f_v : G \to V \) given by \( g \mapsto g \cdot v \). Since \( V \)-valued functions on \( G \) are canonically identified with \( \text{Fun}(G) \otimes V \), we can pair \( \lambda \) with \( f_v \) to obtain

\[
\lambda \cdot v := \lambda(f_v) \in V.
\]

Conversely, if \( V \) is a \( \text{Dist}(G) \)-module then the corresponding \( G \)-action is defined by

\[
g \cdot v = \delta_g \cdot v.
\]
2 The sum of squares theorem

We recall for the reader’s convenience the statement of Theorem III.2.3. For the rest of these notes we work over \( \mathbb{C} \).

**Theorem 2.1.** Let \( G \) be a finite group and \( V_1, \cdots, V_r \) its irreducible representations up to isomorphism. Then we have

\[
\# G = (\dim V_1)^2 + \cdots + (\dim V_r)^2.
\]

**Proof.** The Artin-Wedderburn structure theorem tells us that the group algebra decomposes into a finite product of matrix algebras over \( \mathbb{C} \). Each factor, being a matrix algebra over a field, has a unique simple module, which must be one of the \( V_i \) (see Exercise 0.6 in Dennis and Farb). Thus

\[
\mathbb{C}[G] \cong \prod_{i=1}^r \text{End}_\mathbb{C}(V_i),
\]

and taking dimensions of both sides yields the desired equation.

3 Characters and the trace pairing

In this section we prove Theorem III.5.5, whose statement we now repeat.

**Theorem 3.1.** The irreducible characters of \( G \) form a basis of \( \text{Fun}(G)^G \).

Recall that \( \text{Fun}(G)^G \) is the space of class functions, i.e. conjugation-invariant functions \( G \to \mathbb{C} \). We explained in Section III.5 that Theorem 3.1 implies Theorem III.2.2, which says that conjugacy classes are noncanonically in bijection with irreducible representations.

We will deduce Theorem 3.1 from a more general result. Let \( A \) be a \( \mathbb{C} \)-algebra.

**Definition 3.2.** The character of a finite-dimensional \( A \)-module \( V \) is the linear map \( \chi_V : A \to \mathbb{C} \) defined by \( \chi_V(a) := \text{tr}(a; V) \).

When \( A = \mathbb{C}[G] \) we recover our previous definition of a character, since \( \chi_V \in \mathbb{C}[G]^* = \text{Fun}(G) \).

If \( A \) itself is finite-dimensional then we may consider the character \( \chi_A : A \to \mathbb{C} \).

**Definition 3.3.** The trace pairing \( A \otimes A \to \mathbb{C} \) on a finite-dimensional \( \mathbb{C} \)-algebra \( A \) is given by \( a \otimes b \mapsto \chi_A(ab) \).

Note that the trace pairing is a symmetric bilinear form on \( A \).

**Proposition 3.4.** The trace pairing on \( A \) is nondegenerate if and only if \( A \) is semisimple.

**Proof.** If \( A \) is semisimple then it decomposes as a product of matrix algebras, so it suffices to show the trace form on \( A = \text{End}(V) \) is nondegenerate for \( V \) a finite-dimensional vector space. We saw that a choice of basis determines a decomposition of \( A \)-modules \( A \cong V^\oplus n \), where \( n = \dim V \). Thus, for any \( \varphi \in A \), we have \( \chi_A(\varphi) = n \text{ tr} \varphi \). So we must show that if \( \varphi \neq 0 \), there exists \( \psi \in A \) such that \( n \text{ tr}(\varphi \circ \psi) \neq 0 \). Indeed, if \( \varphi \) has nonzero \((i,j)\) entry with respect to some basis, let \( \psi \) correspond to the matrix with 1 in the \((j,i)\) entry and 0’s elsewhere.

The converse requires a bit of machinery that we haven’t developed, and we won’t need it to prove Theorem 3.1. Let’s give the argument anyway because it leads to an alternative proof of Maschke’s theorem. It suffices to show that the Jacobson radical \( J(R) = 0 \) by Theorem 2.2 in Dennis and Farb. By Theorem 2.4 in loc. cit. any element \( j \in J(R) \) is nilpotent, and in particular \( aj \) is nilpotent for any \( a \in A \). Thus \( aj \) acts nilpotently on \( A \), which implies that \( \chi_A(aj) = 0 \) (a nilpotent operator can be realized as a strictly upper triangular matrix in some basis). By nondegeneracy of the trace pairing this implies that \( j = 0 \) as desired.

Now we can give yet another proof of Maschke’s theorem, this time without averaging.
Corollary 3.4.1. The algebra \( \mathbb{C}[G] \) is semisimple.

Proof. It suffices to show that the trace pairing on \( A = \mathbb{C}[G] \) is nondegenerate. For \( g \in G \) we have

\[
\chi_A(g) = \begin{cases} \# G & \text{if } g = e, \\ 0 & \text{if } g \neq e. \end{cases}
\]

This follows from Exercise III.5.4 by counting fixed points. Now suppose \( \sum_{g \in G} x_g g \in A \) is in the kernel of the trace pairing, meaning

\[
\chi_A(a \sum_{g \in G} x_g g) = 0
\]

for all \( a \in A \). But for any \( g \in G \) we can put \( a = g^{-1} \), so the relation above becomes \( \# G \cdot c_g = 0 \). Thus \( c_g = 0 \) for all \( g \in G \).

Let \([A, A] \subset A\) denote the span of the commutators \([x, y] := xy - yx, x, y \in A\). This is generally just a subspace, not an ideal. The vector space \( C(A) := A/[A, A] \) is called the cocenter of \( A \).

Proposition 3.5. If \( A \) is semisimple, then the trace pairing induces a linear isomorphism

\[
Z(A) \rightarrow C(A)^*.
\]

Proof. By Proposition 3.4 it suffices to show that \([A, A] = Z(A)^{\perp}\) with respect to the trace pairing. As usual everything is compatible with finite products, and we may assume that \( A = \text{Mat}_n(\mathbb{C}) \) for some \( n \geq 1 \). First we show that

\[ [A, A] = \mathfrak{sl}_n(\mathbb{C}) := \{ B \in \text{Mat}_n(\mathbb{C}) \mid \text{tr } B = 0 \}. \]

By standard properties of the trace we have \( \mathfrak{sl}_n(\mathbb{C}) \subset [A, A] \). For any \( 1 \leq i, j \leq n \) denote by \( E_{ij} \in A \) the matrix with 1 in the \((i, j)\) entry and 0’s elsewhere. Note that the collection

\[ \{ E_{ij} \mid 1 \leq i \neq j \leq n \} \cup \{ E_{ii} - E_{i+1,i+1} \mid 1 \leq i < n \} \]

is a basis of \( \mathfrak{sl}_n(\mathbb{C}) \). Now \([A, A] \subset \mathfrak{sl}_n(\mathbb{C})\) follows from the identities

\[ [E_{ik}, E_{kj}] = E_{ij} \text{ for } i \neq j \]

and

\[ [E_{i,i+1}, E_{i+1,i}] = E_{ii} - E_{i+1,i+1}. \]

It remains to prove that \( \mathfrak{sl}_n(\mathbb{C}) = Z(A)^{\perp} \). Recall that \( Z(A) = \mathbb{C} \), so

\[ Z(A)^{\perp} = \{ B \in \text{Mat}_n(\mathbb{C}) \mid z \text{ tr } B = z \text{ tr}(zB) = 0 \text{ for all } z \in \mathbb{C} \} = \mathfrak{sl}_n(\mathbb{C}). \]

By elementary properties of the trace, the characters of finite-dimensional \( A \)-modules belong to \( C(A)^* \).

Corollary 3.5.1. If \( A \) is semisimple, then the characters of the simple \( A \)-modules form a basis of \( C(A)^* \).

Proof. Let \( V_1, \ldots, V_r \) be the simple \( A \)-modules up to isomorphism and \( \chi_1, \ldots, \chi_r \) the corresponding characters. This determines a decomposition

\[ A \cong \prod_{i=1}^r \text{End}_\mathbb{C}(V_i). \]

Let \( e_i \in Z(A) \) be the element that acts by the identity on \( V_i \) and by 0 on \( V_j \) for \( j \neq i \), so that \( e_1, \ldots, e_r \) is a basis of \( Z(A) \). We claim that the trace pairing sends this basis to \( \dim V_1 \cdot \chi_1, \ldots, \dim V_r \cdot \chi_r \), which will imply that the latter is a basis and hence so is \( \chi_1, \ldots, \chi_r \). One computes

\[ \chi_A(e_i a) = \text{tr}(a; \text{End}_\mathbb{C}(V_i)) = \dim V_i \cdot \text{tr}(a; V_i) = \dim V_i \cdot \chi_i(a). \]
Now we specialize to the case $A = \mathbb{C}[G]$. The theorem is almost immediate.

**Proof of Theorem 3.1.** In view of Corollary 3.5.1, it suffices to observe that $C(A)^*$ is canonically identified with the space of class functions $\text{Fun}(G)^G$. Because $C(A)$ is a quotient of $A$, dually $C(A)^*$ is a subspace of $A^* = \text{Fun}(G)$. It is an exercise to verify that for $\lambda \in A^*$, the condition $\lambda(ab - ba) = 0$ for all $a, b \in A$ is equivalent to $\lambda(xy^{-1}) = \lambda(x)$ for all $x, y \in G$.

\[\Box\]

4 Algebraic integers and the divisibility theorem

In this section we prove Theorem III.2.4, whose statement we now recall.

**Theorem 4.1.** If $G$ is a finite group and $V$ is an irreducible representation of $G$, then $\dim V$ divides $\#G$.

The proof of Theorem 4.1 proceeds by a tricky number-theoretical argument using the notion of integrality.

**Definition 4.2.** A number $\alpha \in \mathbb{C}$ is called an algebraic integer if $\alpha$ is a root of a monic polynomial with integer coefficients.

The idea is to somehow show that the rational number $\frac{\#G}{\dim V}$ is an algebraic integer, and then the next result will imply that it is an ordinary integer.

**Proposition 4.3.** A rational number is an algebraic integer if and only if it is an integer.

**Proof.** Any $n \in \mathbb{Z}$ is the root of $x - n$. For the converse, suppose $\frac{m}{n} \in \mathbb{Q}$, $m$ and $n$ relatively prime, is a root of the monic polynomial

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0.$$ Substituting and clearing denominators, we obtain

$$mn^d + a_{d-1}mn^{d-1}n + \cdots + a_1mn^{d-1} + a_0n^d = 0.$$ Thus $n$ divides $m^d$, so we must have $n = \pm 1$.

\[\Box\]

More generally, if $R$ is any ring, we can speak of elements integral over $\mathbb{Z}$ (from now on just integral), which satisfy monic polynomials with coefficients in $\mathbb{Z}$. Clearly this property is preserved under application of ring homomorphisms.

**Proposition 4.4.** An element $r \in R$ is integral if and only if $r$ is contained in a subring $S \subset R$ which is finitely generated as an abelian group. If $R$ is commutative then the set of integral elements forms a subring.

**Proof.** If $r \in R$ is integral then let $S$ be the subring of $R$ generated by $r$, i.e. the image of the homomorphism $\mathbb{Z}[x] \rightarrow R$ which sends $x \mapsto r$. If $r$ satisfies a monic integral polynomial of degree $d$, then we claim that $S$ is generated as an abelian group by $1, r, r^2, \ldots, r^{d-1}$. This is because $r^d$ is a $\mathbb{Z}$-linear combination of these elements, so any integral polynomial in $r$ reduces to one of degree strictly less than $d$.

Conversely, suppose that $r \in S \subset R$, where $S$ is a subring whose additive group is finitely generated. We can assume that $S$ is commutative by replacing $S$, if necessary, with the subring generated by $r$. Consider the group endomorphism of $S$ given by left multiplication by $r$. Choosing a set of generators $s_1, \ldots, s_n$ for $S$ as a group, the action of $r$ can be represented by a matrix $A \in \text{Mat}_n(\mathbb{Z})$, whose coefficients satisfy

$$rs_i = \sum_{j=1}^n a_{ij} s_j.$$ That is, the matrix $rI - A \in \text{Mat}_n(S)$ annihilates $(s_1, \ldots, s_n) \in S^n$. This immediately implies that $\det(rI - A) \in S$ annihilates $S$, but then

$$\det(rI - A) = \det(rI - A) \cdot 1 = 0.$$
Thus \( \det(xI - A) \in \mathbb{Z}[x] \) is the desired monic polynomial.

Now suppose that \( R \) is commutative and \( r, s \in R \) are integral. The subalgebras generated by \( r \) and \( s \) are generated as groups by \( 1, r, \cdots, r^{m-1} \) and \( 1, s, \cdots, s^{n-1} \) for some \( m, n \geq 0 \). Then the subring generated by \( r \) and \( s \) (the image of the homomorphism \( \mathbb{Z}[x, y] \to R \) which sends \( x \mapsto r \) and \( y \mapsto s \)) is generated as a group by

\[ \{ r^i s^j \mid 0 \leq i < m, 0 \leq j < n \}. \]

This proves in particular that \( r + s \) and \( rs \) are integral.

Our argument involves expressing \( \frac{\# G}{\dim V} \) in terms of character values, so we must first show that the latter are algebraic integers.

**Proposition 4.5.** If \( V \) is a finite-dimensional representation of a finite group \( G \) then \( \chi_V \) takes algebraic integer values.

**Proof.** We claim that any \( g \in G \) must act by a diagonalizable operator with all its eigenvalues roots of unity. If \( g \mapsto \varphi \) then \( \varphi^n = \text{id}_V \) for some \( n \geq 1 \), so \( \varphi \) defines a representation of \( \mathbb{Z}/n\mathbb{Z} \) on \( V \). The latter is a finite abelian group, so \( V \) splits into a sum of one-dimensional \( \mathbb{Z}/n\mathbb{Z} \)-representations, i.e. eigenspaces for \( \varphi \). The relation \( \varphi^n = \text{id}_V \) immediately implies that all eigenvalues of \( \varphi \) are roots of unity.

Thus \( \chi_V(g) \) is a sum of roots of unity. Roots of unity are algebraic integers because they are roots of the monic polynomial \( x^n - 1 \) for some \( n \geq 1 \), and Proposition 4.4 shows that sums of algebraic integers are algebraic integers.

We are finally ready to tackle the proof of Theorem 4.1. We follow the argument of Etingof et al. from *Introduction to representation theory*.

**Proof of Theorem 4.1.** List the conjugacy classes \( C_1, \cdots, C_r \) in \( G \), and put \( \delta_i = \sum_{x \in C_i} x \) for each \( 1 \leq i \leq n \). Observe that \( \delta_i \) is central in \( \mathbb{C}[G] \):

\[ \delta_i g = \sum_{x \in C_i} x g = \sum_{x \in C_i} g x = g \delta_i. \]

Thus, by Schur’s lemma, it must act by a scalar \( \lambda_i \) on the irreducible representation \( V \). In fact, \( \lambda_i \) is an algebraic integer: the ring \( \mathbb{Z}[G] \) has a finitely generated additive group so the \( \delta_i \in \mathbb{Z}[G] \) are integral by Proposition 4.4. Since the \( \lambda_i \) are the images of the \( \delta_i \) under a ring homomorphism, namely the action of \( \mathbb{Z}[G] \subset \mathbb{C}[G] \) on \( V \), they are algebraic integers.

On the other hand, we can explicitly compute the \( \lambda_i \) by taking traces:

\[ \lambda_i = \frac{1}{\dim V} \text{tr}(\delta_i; V) = \frac{1}{\dim V} \sum_{x \in C_i} \chi_V(x) = \frac{\# C_i}{\dim V} \chi_V(x_i), \]

where \( x_i \in C_i \) is a fixed representative. Applying the orthogonality relation \( \langle \chi_V, \chi_V \rangle = 1 \) and regrouping, we obtain

\[ \frac{\# G}{\dim V} = \frac{1}{\dim V} \sum_{x \in G} \chi_V(x) \chi_V(x^{-1}) = \sum_{i=1}^r \frac{\# C_i}{\dim V} \chi_V(x_i) \chi_V(x_i^{-1}) = \sum_{i=1}^r \lambda_i \chi_V(x_i^{-1}). \]

Since the \( \lambda_i \) are algebraic integers, and so are the \( \chi_V(x_i^{-1}) \) by Proposition 4.5, Proposition 4.4 implies that the right hand side is an algebraic integer. But \( \frac{\# G}{\dim V} \) is also rational, so apply Proposition 4.3 to finish the proof.